S. Hrg. 118–028

PROTECTING OUR CHILDREN ONLINE

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

FEBRUARY 14, 2023

Serial No. J-118-3

Printed for the use of the Committee on the Judiciary



PROTECTING OUR CHILDREN ONLINE

S. Hrg. 118–028

PROTECTING OUR CHILDREN ONLINE

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

FEBRUARY 14, 2023

Serial No. J-118-3

Printed for the use of the Committee on the Judiciary



52–253 PDF

U.S. GOVERNMENT PUBLISHING OFFICE WASHINGTON : 2023

COMMITTEE ON THE JUDICIARY

RICHARD J. DURBIN, Illinois, Chair

DIANNE FEINSTEIN, California SHELDON WHITEHOUSE, Rhode Island AMY KLOBUCHAR, Minnesota CHRISTOPHER A. COONS, Delaware RICHARD BLUMENTHAL, Connecticut MAZIE K. HIRONO, Hawaii CORY A. BOOKER, New Jersey ALEX PADILLA, California JON OSSOFF, Georgia PETER WELCH, Vermont

LINDSEY O. GRAHAM, South Carolina, Ranking Member CHARLES E. GRASSLEY, Iowa JOHN CORNYN, Texas MICHAEL S. LEE, Utah TED CRUZ, Texas JOSH HAWLEY, Missouri TOM COTTON, Arkansas JOHN KENNEDY, Louisiana THOM TILLIS, North Carolina MARSHA BLACKBURN, Tennessee

JOSEPH ZOGBY, Chief Counsel and Staff Director KATHERINE NIKAS, Republican Chief Counsel and Staff Director

$\rm C\,O\,N\,T\,E\,N\,T\,S$

FEBRUARY 14, 2023, 11:03 A.M.

STATEMENTS OF COMMITTEE MEMBERS

	Page
Durbin, Hon. Richard J., a U.S. Senator from the State of Illinois	1
Graham, Hon. Lindsey O., a U.S. Senator from the State of South Carolina	3
Blumenthal, Hon. Richard, a U.S. Senator from the State of Connecticut	4
Blackburn, Hon. Marsha, a U.S. Senator from the State of Tennessee	5

WITNESSES

Witness List	45
Bride, Kristin, survivor parent and social media reform advocate, Portland,	
Oregon	8
prepared statement	46
DeLaune, Michelle C., president and chief executive officer, National Center	
for Missing & Exploited Children, Alexandria, Virginia	10
prepared statement	53
Golin, Josh, executive director, Fairplay, Boston, Massachusetts	15
prepared statement	73
Lembke, Emma, founder, Log Off Movement, Birmingham, Alabama	9
prepared statement	93
Pizzuro, John, chief executive officer, Raven, Point Pleasant, New Jersey	12
prepared statement	96
Prinstein, Mitch J., Ph.D., ABPP, chief science officer, American Psychological	
Association, Washington, DC	14
prepared statement	103

QUESTIONS

Questions submitted to Kristin Bride by Senator Whitehouse	125
Questions submitted to Michelle C. DeLaune by:	
Senator Whitehouse	126
Senator Tillis	127
Questions submitted to Josh Golin by:	
Senator Whitehouse	128
Senator Tillis	129
Questions submitted to Emma Lembke by Senator Whitehouse	131
Questions submitted to John Pizzuro by:	
Senator Whitehouse	132
Senator Welch	133
Senator Tillis	134
Questions submitted to Mitch J. Prinstein by:	
Senator Whitehouse	135
Senator Welch	136

ANSWERS

Responses of Kristin Bride to questions submitted by Senator Whitehouse	137
Responses of Michelle C. DeLaune to questions submitted by:	
Senator Whitehouse	141

	Page
Responses of Michelle C. DeLaune to questions submitted by-Continued	
Senator Tillis	143
Responses of Josh Golin to questions submitted by:	
Senator Whitehouse	147
Attachment	150
Senator Tillis	200
Responses of Emma Lembke to questions submitted by Senator Whitehouse	207
Responses of John Pizzuro to questions submitted by:	
Senator Whitehouse	209
Senator Welch	210
Senator Tillis	211
Responses of Mitch J. Prinstein to questions submitted by:	
Senator Whitehouse	212
Senator Welch	213

MISCELLANEOUS SUBMISSIONS FOR THE RECORD

Submitted by Chair Durbin:	
Bronstein, Rosellene, statement, February 14, 2023	21
Charmaraman, Linda, Ph.D., statement, February 14, 2023 22	24
	29
Attachment I 23	32
	34
	36
Howard, Ed, letter, February 12, 2023 24	40
Lembke, Anna, M.D., statement, February 14, 2023 24	
RAINN, letter, February 21, 2023 28	57
Submitted by Ranking Member Graham:	
	60
Bergman, Matthew P., Lewis & Clark Law Review, Vol. 26.4, 2023,	
article	62
Bergman, Matthew P., statement, February 14, 2023 30	06

IV

PROTECTING OUR CHILDREN ONLINE

TUESDAY, FEBRUARY 14, 2023

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

The Committee met, pursuant to notice, at 11:03 a.m., in Room 216, Hart Senate Office Building, Hon. Richard J. Durbin, Chair of the Committee, presiding.

Present: Senators Durbin [presiding], Whitehouse, Klobuchar, Coons, Blumenthal, Hirono, Ossoff, Welch, Grassley, Graham, Cornyn, Lee, Hawley, Kennedy, and Blackburn.

Also present: Former Congressman Dick Gephardt and Governor Maura Healey, of Massachusetts.

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

Chair DURBIN. This meeting of the Senate Judiciary Committee will come to order. Before we begin, I want to comment on last night's mass shooting at Michigan State University that took the lives of three students and injured five others. This was the 67th mass shooting in America so far this year. Sixty-seven. More than one a day. Today, February 14th, is already the anniversary of two horrific mass shootings in Parkland, Florida, 5 years ago, and Northern Illinois University in DeKalb, 15 years ago. Now the friends and families of Michigan State students join in that grief. My heart goes out to them.

Last Congress, this Committee held 11 hearings on our Nation's gun violence epidemic, and the Senate passed the most significant gun safety reform in nearly 30 years, but it's not enough. We have more to do. We've lost 5,200 Americans to gunfire already this year, and we're only halfway through February. We were able to come together on a bipartisan basis last year to close gaps in our laws to help reduce shootings. We need to continue the efforts in this Committee and this Congress, and I'll work to do so. We owe that to the families and communities who have lost so much.

Today, the Senate Judiciary Committee will focus on an issue that impacts every family: keeping our kids safe in the internet age. This little device here [holding up a cell phone] is an amazing source of information and communication, but it also has some properties, which we'll discuss today, that are not obvious as you glance at it. Why is it that children who can't really walk on their own, maybe not even talk yet, can operate one of these, can punch the screen to move things? There is a captivation that's taking place there in the minds of young people that continues. It is addictive. We know that. We also know that it's threatening, and we're going to hear some stories today, tales of terrible results of communication through this device.

The online world offers tremendous opportunities and benefits, but it's a serious risk and danger to our kids. In almost every aspect of the real world, child safety is a top priority. We lock the door and teach our kids not to talk to strangers, but in the virtual world, criminals and bullies don't need to pick a lock or wait outside the playground to hurt our kids. They only have to lurk in the shadows online of Facebook and Snapchat. In those shadows, they can bully, intimidate, addict, or sexually exploit our kids right in our own homes. I'd like to turn to a brief video at this point about the risks our children face.

[Video presentation is shown.]

The online exploitation of children is an urgent, growing threat. A report last year from Pew Research found that nearly half of American teens report being harassed or bullied online. Nearly half. As too many families know, cyberbullying, which is often relentless, cruel, and anonymous, can lead to tragic results. Social media can also cause a variety of mental health problems in teenagers, including anxiety, depression, stress, body image issues. This has been well documented, and the Big Tech companies know it.

But despite all these known risks and harms, online platforms are doing everything they can to keep our kids' eyes glued to the screens. In the process, they're vacuuming up tons of data they can use to build profiles and target our kids with even more ads and content. It's a lucrative business at the expense of our kids' privacy, safety, and health. We don't have to take it.

Today we'll hear from an outstanding panel of witnesses about the challenges to protecting kids online and the steps we in the Senate and this Committee can take to help. I want to thank our witnesses Kristin Bride and Emma Lembke who've been personally impacted by this issue. They speak on behalf of many others, and they advocate for change to help spare others what they and their families have gone through. Thank you both for being here today.

I want to acknowledge Rose Bronstein from Chicago who is in the audience. She lost her son Nate to suicide last year after he was viciously bullied over Snapchat and other social media platforms. Ms. Bronstein, I'm sorry for your loss.

We're also joined by experts representing the National Center for Missing & Exploited Children, law enforcement, the American Psychological Association, and the advocacy organization Fairplay. The Big Tech platforms are not here today, but don't worry, they'll have their chance. We'll invite their leaders to appear before this Committee soon to discuss how they can be part of the solution instead of the problem.

Today's discussion builds upon years of important work by this Committee. Ranking Member Graham held important hearings on this issue when he chaired the Committee. I thank him for his partnership in organizing today's hearings. We consider it a bipartisan call to action.

There are a number of worthwhile legislative proposals to protect our kids, such as the EARN IT Act, which enjoys strong bipartisan support in this Committee. Additionally, for months I've been working on a comprehensive bill to close the gaps in the law and crack down on the proliferation of child sex abuse material online, the Stop CSAM Act. Today I'll be releasing a discussion draft of this legislation, and I hope to move forward with it soon.

I also want to acknowledge—she's here now, both Senators are here now—Senators Blumenthal and Blackburn of this Committee, who have been leaders on this issue in another Committee, the Commerce Committee, for a long time. I look forward to hearing our witnesses' ideas for reform, and I hope they can provide the basis for advancing legislation.

Like we do in the real world, we need to protect our kids in the virtual world. This is not a partisan issue. It's an issue that keeps parents and children up at night. It deserves the attention of this Committee and this Congress, and it deserves action. I now turn to the Ranking Member, Senator Graham.

OPENING STATEMENT OF HON. LINDSEY O. GRAHAM, A U.S. SENATOR FROM THE STATE OF SOUTH CAROLINA

Senator GRAHAM. Thank you, Mr. Chairman. One, I want to congratulate you for calling this hearing. It couldn't come at a better time. It's a great panel. I want the people testifying to understand that we're all listening to you, that all of our ears are open and our hearts are open to try to find solutions.

This is the one thing I think unites most Americans, is that most of them feel helpless. The American consumer is virtually unprotected from the adverse effects of social media. That needs to, and I think will, change. How do you protect the consumer?

Well, you have regulatory agencies that protect our food and our health, in general. In this space, there are none. You have statutory schemes to protect the consumer from abuse. In this space, there are none. You can always go to court in America, if you feel like you've been wronged, except here.

So, the American consumer is virtually unprotected from the abuses of social media. And, of all Americans, I think young people are the most exposed here. Parents feel helpless. There's somebody affecting your kids you'll never see, and a lot of times it's a machine. Who's watching the machine, if at all?

And the Surgeon General issued a report that's pretty damning, about the business model is to get people to watch things as much as possible, whether or not those things are good for you. They make money based on eyeballs and advertising. There is no regulatory agency in America with any meaningful power to control this. There are more bills being introduced in this area than any subject matter that I know of. All of them are bipartisan.

So, I want to add a thought to the mix, Mr. Chairman. I'm working with Senator Elizabeth Warren from Massachusetts. We have pretty divergent political opinions, except here. We have to do something, and the sooner, the better. We're going to approach this from consumer protection. We're going to look at a digital regulatory commission that would have power to shut these sites down if they're not doing best business practices to protect children from sexual exploitation online. There were 21 million episodes last year of sexual exploitation against children. It was a million—1.4, I think, in 2014. This is an epidemic. It is a mental health crisis, particularly for young teenaged girls. And we have no system in place to empower parents and empower consumers to seek justice, to fight back, and protect themselves. That's going to change in this Congress, I hope.

So, Mr. Chairman, I look forward to working with you. I know Senator Blackburn's been very involved in the privacy space. I've worked with Senator Blumenthal on the EARN IT Act. So, we're going to work together the best we can to find solutions to empower consumers who are pretty much at the will of social media, and some people are having their lives ruined. It's now time for us to act.

Chair DURBIN. Thanks, Senator Graham. I'm going to ask our two colleagues Senator Blumenthal and Senator Blackburn to give brief opening remarks. As I mentioned earlier, they've both been pioneers in this subject matter.

Senator Blumenthal.

OPENING STATEMENT OF HON. RICHARD BLUMENTHAL, A U.S. SENATOR FROM THE STATE OF CONNECTICUT

Senator BLUMENTHAL. Thanks very much, Mr. Chairman. And I want to personally thank you not only for having this hearing but your very important interest and work on protecting kids online. And I'm grateful, as well, to Senator Graham for his partnership on the EARN IT Act. This cause is truly bipartisan, which Senator Blackburn and I, I think, are showing in real time here, the work that we're doing together. The EARN IT Act can be a meaningful step toward reforming this unconscionably excessive Section 230 shield to Big Tech accountability.

I think we need to be blunt, from the beginning, because we know right now the central truth. Big Tech has relentlessly, ruthlessly pumped up profits by purposefully exploiting kids' and parents' pain. Young people like Emma Lembke have been victims of Big Tech's hideous experiment, as President Biden rightfully called it. Parents like Kristin Bride have lost beautiful children like Carson. Parents whose tears and raw grief as you came to see me in my office have moved me with heartbreaking power.

But beyond heartbreak, what I feel is outrage: outrage at inaction, Congress' inexcusable failure to pass the bill that you advance courageously and eloquently, the Kids Online Safety Act; outrage at Big Tech, pillaging the public interest with its armies of lobbyists and lawyers, despite their pledges of collaboration; outrage that you and other victims must relive the pain and grief that break our hearts and should, finally, be a moral imperative to action.

We came so close, last session. We need to seize this moment. We face a public health imperative, not just a moral reckoning. Our Nation is in the midst of a mental health crisis. If you have any doubt about it, read the latest CDC survey that says three out of five girls in America experience deep depression, sadness, and helplessness that drives many of them to plan suicide.

It's a public health emergency, egregiously and knowingly exacerbated by Big Tech; aggravated by toxic content on eating disorders, bullying, even suicide; driven by Big Tech's black-box algorithms, leading children down dark rabbit holes. We have to give kids and parents—yes, both kids and parents—the tools, transparency, and guardrails they need to take back control over their own lives. And that is why we must and we will double down on the Kids Online Safety Act.

After five extensive hearings last session with Senator Blackburn at our Commerce Consumer Protection Subcommittee, and I thank Senator Maria Cantwell for her leadership; after deeply painful conversations with young people and parents like Emma and Kristin; after testimony from brave whistleblowers like Frances Haugen, who presented documents, not just personal anecdotes, but smoking-gun proof that Facebook calculatingly drove toxic content to draw more eyeballs, more clicks, more dollars, more profits; after Facebook hid this evidence from parents, even misled us, in Congress—it's Big Tobacco's playback and playbook, all over again—the evidence of harm is heartbreakingly abundant beyond any reasonable doubt. Action is imperative now, and I think these brave victims at our hearing ought to provide the impetus and momentum.

Right now, urgently, the Kids Online Safety Act can be a model for how bipartisan legislating can still work, a message to the public that Congress can still work. We need to reform Section 230. Senator Graham and I are working on the EARN IT Act. I commit that we will work on major Section 230 reform, and it will be bipartisan. This mental health crisis will persist, take more young lives, unless Congress cares more about the Kids Online Safety Act than it does about Big Tech.

It's urgent that we move forward and I am haunted by what one parent told me, and all of us, in advocating for the Kids Online Safety Act. She said, "Congress must act. It's a powerful call to action." And she asked, "How many more children have to die before we make them a priority? Now is the time. Let's pass it." That's her quote. Mine is, "Congress needs to act and heed that call and do it now." Thank you, Mr. Chairman.

Chair DURBIN. Thank you, Senator Blumenthal.

Senator Blackburn.

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

Senator BLACKBURN. Thank you, Mr. Chairman. Thank you for calling the hearing today. Appreciate that you and Senator Graham are turning attention to this. As many of you in the audience know, this is something that Senator Blumenthal and I have worked on for quite a period of time. We started on this about 3 years ago, and what you saw over the last couple of years was a series of hearings and Kristin and Emma and others who came in to tell their stories and to provide us with information and to walk us through what was happening.

So, we have heard from parents and kids and teachers and pediatricians and child psychologists who are all looking at us and saying, "This is an emergency." And anybody who doubts it—Senator Blumenthal just held up, and I have also, the CDC report that just came out, where you talk about youth risk behavior. And guess what? Social media is one of those items that is a part of that risk. And we have just taken to heart—we've listened to not only the testimony in the hearings but to many of you that came separately to our offices to talk to us and to say, "This is our experience, and we want somebody to know about this, because something needs to be done."

It is almost as if these social media platforms are operating in the days of the Wild West, and anything goes. And when these children are on these platforms, they're the product. They're the product. Their data is taken. That data is monetized, and then it is sold to the advertisers, who are going to feed more information to these children.

And we've come up with this Kids Online Safety Act. Now, we got close last time, and we almost got it through the finish line, and we didn't. So, new Congress. A new start on this. And we're so pleased that Judiciary Committee is working with us, with Commerce Committee, and we hope to get it on—there are some things that ought to be a given. These social media platforms ought to be required to make these platforms safer by default, not just safer if you go through the 20 next steps, but safer by default. That ought to be required.

We should also have a requirement that these platforms have to do independent audits, go through independent audits, not their research. Now, some of you have said, in these hearings we've done, and you've heard these social media companies say, "Well, we're always auditing ourselves." But who ever knows what that audit shows? Not you. Not me. Nobody knows. They like to keep that to themselves, because as Senator Blumenthal has said, eyeballs on that site for a longer period of time—it's more money, money, money in the bank. And who pays that price? Our kids. Our kids.

Our legislation was supported by 150 different groups. Now, in a time where politics is divided and you hear left and right, to get 150 different groups to come together and support something, I think that's a pretty good day. I think that shows a lot of support. So, we realized that much of the reason these groups were coming out and supporting the transparency and the accountability and the duty of care was because they realized talking to these social media platforms was like talking to a brick wall. They could not get a response, and because of that, something different was going to have to be done.

Senator Graham said it well in his comments. It is imperative that we take an action because this is a health emergency. If you don't believe it, read the CDC report. When you have a majority of children that are experiencing adverse impacts from social media platforms, you have to step in and do something. And that is what we are working to do. We welcome all of you. Thank you to our witnesses, and we look forward to the hearing today.

Chair DURBIN. Thank you, Senator Blackburn. Let me say at the outset that, to explain to any newcomers, we have two roll call votes that are going to start in just a matter of minutes. So, Members will come and go. That is no disrespect to the subject matter or to our witnesses and guests, but we are going to do a tag team to make sure there is always someone here to follow your testimony and try to gather after the roll calls, but that's the circumstance.

Let me welcome the six witnesses. Kristin Bride is a survivor parent to Carson Bride, and she is a nationally recognized social media reform advocate, founding member of the Screen Time Action Network Online Harms Prevention group. She advocates for online safety for kids. A member of the Council for Responsible Social Media, she collaborates with other organizations to raise awareness and advocate legislation to hold Big Tech accountable.

Emma Lembke. She's from Birmingham, Alabama. Second-year political science major at Washington University in St. Louis and the founder of Log Off, a youth movement that works to uplift and empower young people to tackle the complexities of social media. Ms. Lembke has also co-founded Tech(nically Politics), a youth lobbying campaign dedicated to advocating greater regulation for Big Tech.

Michelle DeLaune is president and chief executive officer of the National Center for Missing & Exploited Children, the first woman to lead this organization. During her two decades at NCMEC, Ms. DeLaune has witnessed firsthand the evolving threats to our kids, including the explosion—explosion—of child sexual exploitation online.

John Pizzuro serves as CEO of Raven, an advocacy group that focuses on protecting kids from exploitation and supporting those who fight for them. Previously, Mr. Pizzuro spent 25 years in the New Jersey State Police, with the last 6 years as commander of their Internet Crimes Against Children Task Force. There, he led a team of 200 individuals and 71 law enforcement agencies. They apprehended over 1,500 people who preyed on innocents.

Dr. Mitch Prinstein—is it Prinstein or Prinstein?

Dr. PRINSTEIN. Prinstein.

Chair DURBIN. Prinstein? Dr. Mitch Prinstein, chief science officer for the American Psychological Association, responsible for leading their scientific agenda. Before assuming this post, he was the John Van Seters Distinguished Professor of Psychology at University of North Carolina-Chapel Hill. His research is focused on adolescent interpersonal experience and psychological symptoms, including depression.

Josh Golin, executive director of Fairplay, the leading independent watchdog of children's media and marketing industries. Fairplay holds companies accountable for their harmful marketing and platform design choices, advocates for policies to protect children online. In his role, Mr. Golin regularly speaks to parents, professionals, and policymakers about how to create a healthier environment.

After we swear in the witnesses, each will have 5 minutes for opening statements. Then Senators will have rounds of questions. So, first let me ask that all the witnesses stand to be sworn in. Please raise your right hand.

[Witnesses are sworn in.]

Chair DURBIN. Let the record reflect that witnesses have answered in the affirmative. Ms. Bride, please, if you will, start our round.

STATEMENT OF KRISTIN BRIDE, SURVIVOR PARENT AND SOCIAL MEDIA REFORM ADVOCATE, PORTLAND, OREGON

Ms. BRIDE. Thank you, Chairman Durbin, Ranking Member Graham, and Members of the Committee. My name is Kristin Bride. I am a survivor parent and social media reform advocate and member of the bipartisan Council for Responsible Social Media. I am testifying here today to bring a face to the harms occurring every day resulting from the unchecked power of the social media industry.

This is my son Carson Bride, with the beautiful blue eyes and amazing smile and great sense of humor, who will be forever 16 years old. As involved parents raising our two sons in Oregon, we thought that we were doing everything right. We waited until Carson was in eighth grade to give him his first cell phone, an old phone with no apps. We talked to our boys about online safety and the importance of never sending anything online that you wouldn't want your name and face next to on a billboard. Carson followed these guidelines, yet tragedy still struck our family.

It was June 2020. Carson had just gotten his first summer job making pizzas, and after a successful first night of training, he wrote his upcoming work schedule on our kitchen calendar. We expressed how proud we were of him for finding a job during the pandemic. In so many ways, it was a wonderful night, and we were looking forward to summer. The next morning, I woke to the complete shock and horror that Carson had hung himself in our garage while we slept.

In the weeks that followed, we learned that Carson had been viciously cyberbullied by his Snapchat friends, his high school classmates who were using the anonymous apps Yolo and LMK on Snapchat to hide their identities. It wasn't until Carson was a freshman in high school that we finally allowed him to have social media, because that was how all the students were making new connections.

What we didn't know is apps like Yolo and LMK were using popular social media platforms to promote anonymous messaging to hundreds of millions of teen users. After his death, we discovered that Carson had received nearly 100 negative, harassing, sexually explicit, and humiliating messages, including 40 in just 1 day. He asked his tormentors to swipe up and identify themselves so they could talk things out in person. No one ever did. The last search on his phone before Carson ended his life was for hacks to find out the identities of his abusers.

Anonymous apps like Whisper, Sarahah, and Yik Yak have a long history of enabling cyberbullying and leading to teen suicides. The critical flaws in these platforms are compounded by the fact that teens do not typically report being cyberbullied. They are too fearful that their phones, to which they are completely addicted, will be taken away or that they will be labeled a snitch by their friends.

Yolo's own policies stated that they would monitor for cyberbullying and reveal the identities of those who do so. I reached out to Yolo on four separate occasions in the months following Carson's death, letting them know what happened to my son and asking them to follow their own policies. I was ignored all four times. At this point, I decided I needed to fight back. I filed a national class action lawsuit in May 2021 against Snap Inc., Yolo, and LMK.

We believe Snap Inc. suspended Yolo and LMK from their platform because of our advocacy; however, our complaint against Yolo and LMK for product liability design defects and fraudulent product misrepresentation was dismissed in the Central District Court of California last month, citing Section 230 immunity. And still, new anonymous apps like NGL and sendit are appearing on social media platforms and charging teens subscription fees to reveal the messenger or provide useless hints.

I speak before you today with tremendous responsibility to represent the many other parents who have lost their children to social media harms. Our numbers continue to grow exponentially, with teen deaths from dangerous online challenges, sextortion, fentanyl-laced drugs, and eating disorders. Let us be clear. These are not coincidences, accidents, or unforeseen consequences. They are the direct result of products designed to hook and monetize America's children.

It should not take grieving parents filing lawsuits to hold this industry accountable for their dangerous and addictive product designs. Federal legislation like the Kids Online Safety Act, KOSA, which requires social media companies to have a duty of care when designing their products for America's children, is long overdue. We need lawmakers to step up, put politics aside, and finally protect all children online. Thank you for this opportunity, and I look forward to answering your questions.

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

Chair DURBIN. Thank you, Ms. Bride.

Ms. Emma Lembke?

STATEMENT OF EMMA LEMBKE, FOUNDER, LOG OFF MOVEMENT, BIRMINGHAM, ALABAMA

Ms. LEMBKE. Hello, everyone. My name is Emma Lembke. I am originally from Birmingham, Alabama, but currently I am a sophomore studying political science at Washington University in St. Louis. I am humbled and honored to be here today.

I created my first social media account, Instagram, in the sixth grade. As a 12-year-old girl, to 12-year-old me, these platforms seemed almost magical, but as I began to spend more time online, I was met with a harsh reality. Social media was not magic. It was an illusion, a product that was predicated on maximizing my attention at the cost of my well-being.

As my screen time increased, my mental and physical health suffered. The constant quantification of my worth through likes, comments, and followers heightened my anxiety and deepened my depression. As a young woman, the constant exposure to unrealistic body standards and harmful recommended content led me toward disordered eating and severely damaged my sense of self.

But no matter the harm incurred, addictive features like autoplay and the endless scroll pulled me back into the online world, where I continued to suffer, and there I remained for over 3 years, mindlessly scrolling for 5 to 6 hours a day. I eventually reached a breaking point in the ninth grade, and I began the long and difficult process of rebuilding my relationship with technology in a healthier way.

Senators, my story is not one in isolation. It is a story representative of my generation, Generation Z. As the first digital natives, we have the deepest understanding of the harms of social media, through our lived experiences, but it is from those experiences that we can begin to build the most promising solutions. It is only when young people are given a place at the table that effective solutions can emerge and safer online spaces can be created. The power of youth voices is far too great to continue to be ignored. Through Log Off, I have engaged with hundreds of kids across

Through Log Off, I have engaged with hundreds of kids across the globe who have shared their experiences of harm with me. I have listened as young people have told me stories of online harassment, vicious cyberbullying, unwanted direct messages. But most powerfully, I have heard as members of my generation have expressed concern not just for our own well-being but for younger siblings, for cousins, and for all those to come after us.

While our stories may differ, we share the frustration of being portrayed as passive victims of Big Tech. We are ready to be active agents of change, rebuilding new and safer online spaces for the next generation. Ten years from now, social media will not be what it is today. It will be what members of my generation build it to be. We want to build it differently. We want to build it right.

I came here today as the representative for those young changemakers, to be the voice not just of those in my generation who have been harmed or who are currently struggling but to be a voice for all of those 12-year-old girls yet to come. The genie is out of the bottle, and we will never go back to a time where social media does not exist, nor should we, but make no mistake, unregulated social media is a weapon of mass destruction that continues to jeopardize the safety, privacy, and well-being of all American youth.

It's time to act. And I urge you, Senators, to take meaningful steps to regulate these companies, not just for our generation and my generation, but with my generation. Integrating youth-lived experiences is essential in the regulatory process in getting it right. Thank you for having me here today, and I look forward to answering your questions.

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

Chair DURBIN. Thank you, Ms. Lembke.

Ms. DeLaune?

STATEMENT OF MICHELLE C. DeLAUNE, PRESIDENT AND CHIEF EXECUTIVE OFFICER, NATIONAL CENTER FOR MISS-ING & EXPLOITED CHILDREN, ALEXANDRIA, VIRGINIA

Ms. DELAUNE. Thank you. Good morning, Chairman Durbin, Ranking Member Graham, and Members of the Committee. My name is Michelle DeLaune, and I am the president and CEO of the National Center for Missing & Exploited Children. NCMEC is a nonprofit organization created in 1984 by child advocates to help find missing children, reduce child sexual exploitation, and prevent child victimization. I am honored to be here today to share NCMEC's perspective on the dangers that are facing children online and how we can work together to address these challenges. We have reached an inflection point in efforts to combat online child sexual exploitation, and we need congressional intervention to pass legislation that I'll be speaking to today.

Last year, NCMEC's CyberTipline received over 32 million reports. These reports contained over 88 million images and videos and other content related to child sexual exploitation. And to put these numbers into perspective, we're averaging 80,000 new reports each day. The internet is global, and unfortunately, so is this crime. Ninety percent of the reports that we received last year related to individuals outside of the United States, and the remaining reports, about 3.2 million, related to U.S. individuals.

The report numbers are staggering, but the quality of reports is often lacking, and there are significant disparities in how companies report. For instance, companies have no duty to report child sex trafficking or online enticement of children. Some companies choose not to report sufficient information for those cases to be properly assessed and investigated, and some companies choose not to submit actual images or the videos actually being reported or any information that could be used to identify a suspect or a victim.

And we're just seeing the tip of the iceberg. Very few companies choose to engage in voluntary measures to detect known child sexual abuse material, and those who do proactively look for that make the most reports. Congress has the opportunity to send a powerful message to victims that they are not powerless to protect themselves and when abuse imagery of themselves has been shared online. Currently, child victims have no recourse if a tech company takes no action to stop, remove, and report sexually explicit imagery in which they are depicted.

At the core of NCMEC's mission is helping children and supporting survivors. And we do a lot to support survivors, but we need Congress to help address the complexities that survivors face in this space. The following legislative measures are urgently needed to support survivors: laws that require that content seized by Federal law enforcement from offenders be sent to NCMEC for victim identification efforts and supporting restitution efforts; laws enabling child victims of extortion and enticement to have immunity when reporting their images to NCMEC; laws enabling minor victims to have legal recourse if a tech company knowingly facilitates the distribution of their sexually abusive imagery; regulations to implement the remedies promised to survivors in 2018 when the Amy, Vicky, and Andy Act was passed by Congress; and laws to make sure that we are using the appropriate words when we're discussing these crimes: "child sexual abuse material," not "child pornography."

And while we struggle to address the current volume and complexity of online child sexual exploitation, additional threats to child safety online are occurring. When a platform implements endto-end encryption, no one, not even the platform itself, has visibility into users exploiting children. We believe in a balance between user privacy and child safety. When tech companies implement end-to-end encryption with no preventive measures built in to detect known child sexual abuse material, the impact on child safety is devastating.

Several of the largest reporting companies have indicated that they will be moving to default end-to-end encryption this year. We estimate that, as a result, two-thirds of reports to the CyberTipline submitted by tech companies will go away, and these reports will be lost simply because tech companies have chosen to stop looking for the material. And we can talk about lost report numbers, but behind every report is a child, and the abuse doesn't stop just because we decide to stop looking for it.

We look forward to working with Congress and other stakeholders on solutions. In closing, NCMEC is proud to support many excellent legislative initiatives from last Congress, including the EARN IT Act, the END Child Exploitation Act, and the Preventing Child Sexual Abuse Act. And we look forward to working with Congress to ensure the legislative measures become law in the current term.

I thank you for the opportunity to appear before the Committee to discuss the protection of children online. We're eager to continue working with this Committee, survivors and their families, the Department of Justice, engaged tech companies, and other nonprofits to find solutions to these problems, because like you, we believe that every child does deserve a safe childhood. I thank you, and I look forward to your questions.

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

Chair DURBIN. Thank you, Ms. DeLaune.

Mr. Pizzuro?

STATEMENT OF JOHN PIZZURO, CHIEF EXECUTIVE OFFICER, RAVEN, POINT PLEASANT, NEW JERSEY

Mr. PIZZURO. Chairman Durbin, Ranking Member Graham, and distinguished Senators, thank you for this opportunity to testify on protecting our children online. Today there are countless victims of infant and children being raped online as well as extortion. The sad reality is we're failing to protect our children from the threats they face online. Those who would protect our youth are overburdened, under-resourced, which makes those children vulnerable.

I'm here today as the CEO of Raven, an advocacy group comprised of 14 professionals, including 9 retired Internet Crimes Against Children commanders, task force commanders who have committed their lives to the advocacy and the protection of children. I'm retired from the New Jersey State Police, where I served as the commander of the ICAC Task Force.

We witnessed children targeted by offenders across all platforms. No social media or gaming platform was safe, from apps such as Snapchat, Twitter, Kik, Telegram, Discord, LiveMe, and MeetMe to gaming platforms and outline games such as Minecraft, Roblox, and Fortnite. And these just represent a fraction of places where offenders regularly interact with children. If the platform allows individuals to chat or a way to share a photograph and videos, I assure you there's a very real danger that offenders are using that access to groom or sexually exploit minors. Children are made vulnerable on these platforms as a result of poor moderation, the absence of age or identity verification, and inadequate or missing safety mechanisms and the sheer determination of offenders. As the New Jersey ICAC commander, I struggled with the significant increases in arrests, victims, investigations we faced each year. These challenges were frustratingly present with every ICAC task force commander throughout the United States. The most staggering increase we faced was self-generated sexual abuse videos of children ages seven, eight, and nine.

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. The details of these cases shock the conscience. There's 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 the age of interest for the offender, or the offender bought a stuffed animal for the 10-year-old that he was going to rape, along with a bottle of Viagra and other sexual devices when that Viagra failed.

Today, law enforcement is no longer able to proactively investigate child exploitation cases, due to the volume of CyberTips. As a result of that increase, law enforcement agencies have been forced to become reactive, and most no longer can engage in the proactive operations such as peer-to-peer file-sharing investigations or undercover chat operations which target hands-on offenders.

Sadly, 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 to desperately identify worthwhile cases.

Peer-to-peer file-sharing investigations and operations used to allow ICAC task forces to efficiently locate and apprehend handson offenders. In the last 90 days alone, there have been 100,000 IP addresses across the U.S. that have distributed known images of rape and toddler sexual abuse, yet only 782, less than 1 percent, are being worked right now.

The Darknet, including Tor, has become the newest online haven for child exploitation. 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. There's a post, even, named The Art of Seduction, that explained how to seduce children, that has been read more than 54,000 times.

Based upon what I have experienced, I can confidently tell you three things. At the moment, the predators are winning, our children are not safe, and those who are fiercely committed to protecting them are drowning and will continue to do so unless we can get them the resources they need. I thank you for the opportunity to testify here today, and I welcome your questions.

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

Chair DURBIN. Thank you very much, Mr. Pizzuro.

Dr. Prinstein?

STATEMENT OF MITCH J. PRINSTEIN, Ph.D., ABPP, CHIEF SCIENCE OFFICER, AMERICAN PSYCHOLOGICAL ASSOCIA-TION, WASHINGTON, DC

Dr. PRINSTEIN. Good morning, Chairman Durbin, Ranking Member Graham, and Members of the Judiciary Committee. Thanks for the opportunity to testify today.

Psychologists are experts in all human behavior, and we have been studying the effects of social media scientifically for years. In my written testimony, I've detailed a variety of caveats, limitations, and clarifications that make it challenging as a scientist to offer causal statements about the effects of social media. In short, online activity likely offers both benefits and harms. Today, I want to discuss specific social media behaviors and features that are most likely to harm and which youth may be most vulnerable.

likely to harm and which youth may be most vulnerable. Unfortunately, some of these most potentially harmful features are built directly into the architecture of many social media applications, and kids are explicitly directed toward them. To date, we have identified at least seven sets of results that deserve more attention to safeguard risk for children. I will briefly describe these here, but first it's critical to understand that, following the first year of life, the most important period for the development of our brains begins at the outset of puberty, and this is precisely the time when many are given relatively unfettered access to social media and other online platforms. In short, neuroscience research suggests that when it comes to seeking attention and praise from peers, adolescents' brains are all gas pedal with weak brakes. This is a biological vulnerability that social media capitalizes on, with seven psychological implications.

First, our data suggest that the average teen is picking up their phone over 100 times and spending over 8 hours online a day, mostly on social media. Psychological science reveals that over half of all youth report at least one symptom of clinical dependency on social media, such as the inability to stop using it or a significant impairment in their ability to carry out even simple daily functions.

Second, as compared to what kids see offline, data suggest that exposure to online content changes how youths' brains respond to what they see and influences teens' later behavior. These are psychological and neuroscientific phenomena occurring outside of youths' conscious awareness, suggesting a potentially troubling link between likes, comments, reposts, and teens' later risk-taking behavior.

Third, although many platforms have functions that can be used to form healthy relationships, users instead are directed to metrics and follower counts that don't really offer psychological benefits. For this reason, social media often offers the empty calories of social interaction that appear to help satiate our biological and social needs but do not contain the healthy ingredients necessary to reap benefits. Research reveals that in the hours following social media use, teens paradoxically report increases, rather than decreases, in loneliness.

Fourth, data suggest that approximately half of youths experience digital stress, a phenomenon resulting from too many notifications across platforms, a fear of missing important social updates, information overload, and anxiety that their posts will be well received. More digital stress predicts increases in depression over time.

Fifth, a remarkably high proportion of teens are exposed to dangerous discriminatory and hateful content online. This predicts anxiety and depression among youth even beyond the effects of similar content they see offline.

Sixth, the more time kids are online, the less time they're engaged in activities critical for healthy development, most notably sleep. Sleep disruptions at this age are associated with changes in the size and physical characteristics of growing brains.

And last, new evidence suggests frequent technology use may change adolescent brain growth to increase sensitivity to peers' attention and change teens' self-control.

So, what do we do? First and foremost, we must increase Federal funding for this research, \$15 million will not move the needle. The funding for this work should be commensurate with our commitment to protect children.

Second, parents and teens must become better educated about these emerging research findings. Recently, more than 150 organizations, led by APA, called on the Surgeon General to create and distribute teaching resources so families could minimize risks and maximize benefits from social media.

Third, more must be done to protect youth who belong to traditionally marginalized communities. Warnings on harmful, illegal, hateful, and discriminatory content should be mandated, yet content in spaces scientifically proven to offer social support and vital health information to members of these communities must be saved.

The manipulation of children to generate a profit is unacceptable. The use of children's data should be illegal, and the use of psychological tactics known to create addiction or implicitly influence children's behavior should be curtailed. Social media companies should be compelled to disclose both internal and independent data documenting potential risks that come from the use of their products, so parents, teens, and regulators can make informed decisions.

APA is heartened by the focus on mental health in Congress and eager to work with this Committee to develop legislation and help enact bills that will protect children. Your actions now can make a difference.

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

Chair DURBIN. Thank you, Doctor. Mr. Golin?

STATEMENT OF JOSH GOLIN, EXECUTIVE DIRECTOR, FAIRPLAY, BOSTON, MASSACHUSETTS

Mr. GOLIN. Thank you, Chair Durbin, Ranking Member Graham, and distinguished Members of the Committee for holding this important hearing. My name is Josh Golin, and I'm executive director of Fairplay, an organization committed to building a world where kids can be kids, free from the harmful manipulations of Big Tech and the false promises of marketers. We advocate for policies that would create an internet that is safe for young people and not exploitative or addictive. You've heard today from witnesses about a litany of online harms that have had a devastating toll on families in our society. These harms share a common nexus: Big Tech's business model and manipulative design choices. Digital platforms are designed to maximize engagement, because the longer they capture a user's attention, the more money they make by collecting data and serving targeted ads. As a result, children are subject to manipulative design and relentless pressure to use these platforms as often as possible.

Over a third of teenagers say they are on social media almost constantly. Overuse of social media displaces critical offline activities like sleep, exercise, offline play, and face-to-face interactions, which, in turn, undermines children's well-being. Big Tech's profitdriven focus on engagement doesn't just harm young people by fostering compulsive overuse. It also exploits their developmental needs, often at the expense of their safety and well-being.

For example, displays of likes and follower counts, which take advantage of young people's desire for social approval, invite harmful social comparisons, and incentivize interactions with strangers and the posting of provocative and risqué content. Additionally, algorithms designed to maximize engagement fill young people's feeds with curated content that is most likely to keep them online, without regard to the user's well-being or potentially harmful consequences.

So, on platforms like Instagram and TikTok, depressed teens are shown content promoting self-harm, and young people interested in dieting are barraged with content promoting eating disorders. A report last year from Fairplay detailed how Meta profits from 90,000 unique pro-eating-disorder accounts on Instagram that reach more than 6 million minors, some as young as nine.

How did we get here? For one, the last time Congress passed a law to protect children online was 25 years ago. The digital landscape has changed dramatically in unforeseen ways since the passage of the Children's Online Privacy Protection Act, and that law only covers children until they turn 13, leaving a significant demographic vulnerable to exploitation and harm. Consequently, the social media platforms that define youth culture and shape our children's values, behavior, and self-image were developed with little to no thought about how young people might be negatively affected.

At this point, it is clear that tech platforms will not unilaterally disarm in the race for children's precious attention, nor can we expect young people to extract themselves from the exploitative platforms where their friends are or expect overworked parents to monitor every moment that their kids are online. We need new legislation that puts the brakes on this harmful business model and curbs dangerous and unfair design practices.

Such legislation should: one, extend privacy protections to teens, to limit the collection of data that fuels harmful recommendations and puts young people at risk of privacy harms; two, ban surveillance advertising to children and teens, to protect them from harmful marketing targeted to their individual vulnerabilities; three, impose liability on companies for how their design choices and algorithms impact young people; four, require platforms to make children's privacy and account settings the most protective by default; and, finally, impose transparency requirements, including access to algorithms, that enable outside researchers to better understand how social media impacts young people. Last Congress, the Kids Online Safety Act and the Children and Teens' Online Privacy Protection Act, two bills which, together, would do all five of these things, advanced out of the Commerce Committee with broad bipartisan support.

The Committee votes followed a series of important hearings in the Senate Judiciary and Commerce Committees, as well as the House, that established a clear record of harm and the need for new online protections for young people. We've named the problem and debated the solution. Now is the time to build on last year's momentum and disrupt the cycle of harm by passing privacy and safety-by-design legislation. Let's make 2023 the year that Congress finally takes a huge step toward creating the internet children and families deserve. Thank you so much for having me here today, and I look forward to your questions.

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

Chair DURBIN. I want to thank all the witnesses. And, as you noticed, some of the Members are going to vote and will return. At the bottom of this discussion, from the legal point of view, is Section 230 of the Communications Decency Act, which I'm sure you're all aware of as to the liability of these companies for the speech that is broadcast or is exercised over their social media. It provides that companies will not be treated as publisher or speaker of any information provided by another person. Gets them off the hook.

The EARN IT Act, which we are debating here, would change that ball game. Unless there is a provable effort by these companies to police their own product, they would be exposed to liability. And I will tell you, as a former trial lawyer, I invite them to take on the media that ignore that responsibility after the EARN IT Act is enacted into law. I hope that will be soon.

Ms. DeLaune, when you told the story about encryption inhibiting the CyberTips that come your way, I couldn't help but be struck by the numbers that you used. Last year, 32 million CyberTips were sent to NCMEC, your organization, concerning child sex abuse material. Upwards of 80 percent, or 25 million, of those would be lost if the companies adopt end-to-end encryption. Would you bring that explanation down to a level where liberal arts majors are with you?

[Laughter.]

Ms. DELAUNE. Absolutely, Senator. Thank you. With the end-toend encryption, again, end-to-end encryption serves a very important purpose. End-to-end encryption with no mitigation strategy for the detection of known child sexual abuse imagery is unacceptable, though what we have seen—the vast numbers for the CyberTipline are because companies have voluntarily—a handful of companies have voluntarily chosen to look and seek out known child sexual abuse material. By simply turning off the lights and no longer looking, the abuse doesn't go away. The abuse continues; just nobody is able to actually investigate, intervene, and help a child.

You know, we really support a balanced approach. There are disagreements and discussions between many stakeholders regarding how end-to-end encryption can balance user safety, user privacy, with not having children as collateral damage. You know, we also want to speak to the privacy of the children who are depicted in the imagery that is continuing to be circulated. These are images, as Mr. Pizzuro mentioned, images of children being sexually abused and raped. They also are entitled to privacy. So, we do look for a balanced approach that will help support user privacy and not leave children as unfortunate collateral damage.

Chair DURBIN. Let me open another subject for inquiry, and that is the statement by Dr. Prinstein, Mr. Golin—kind of reflects, Emma Lembke, on your decision at a very young age to do something about what you consider to be a problem. I'm trying to square this, the possibility of diverting people from conduct which apparently is almost addictive in its nature and move them to a different level. Can you comment on that?

Ms. LEMBKE. Yes, sir. And, Senator, thank you for your question. I think what is important to note is that social media is not all bad. Members of my generation understand it to be a multifaceted entity, one where we can connect with each other, we can explore our identities, and we can express ourselves on a new dimension.

The difficulty, though, of reaping these benefits in these online spaces is, as they are right now, as the status quo creates it, I, a 12-year-old girl, could go onto Instagram and research a healthy recipe and within seconds be fed pro-anorexic content. There are steps that companies can take to place meaningful safeguards so that this content does not harm young people and so that we can begin to go into these online spaces in a safer and more productive manner, reaping the benefits of a technological era.

Chair DURBIN. Dr. Prinstein, your comment on that?

Dr. PRINSTEIN. I agree. The adolescent brain is built to develop dopamine and oxytocin receptors in an area of the brain that makes us want to connect with peers, and it feels really good when we do. The area of the brain that stops us from engaging in impulsive acts, called the prefrontal cortex, does not fully develop until the age of 25. So, from 10 to 25, kids' brains are built in such a way to make them crave the exact kind of content that social media can provide with like buttons and reposts, but they are biologically incapable of stopping themselves from incessant use of these platforms. That vulnerability is being exploited by these platforms.

Chair DURBIN. And the question is whether or not, on their own, kids can solve the problem. Do they need help?

Dr. PRINSTEIN. They need help.

Chair DURBIN. What kind of help?

Dr. PRINSTEIN. Reminders telling kids that they've been on for longer than they intended; helping kids to stop—the signals that are coming through social media in the forms of likes, reposts, algorithms that are showing them content, feeding them the next video, feeding them the next post—those are all actually making things much worse, from a neuroscientific perspective. If there were controls in place, that were age based, to make sure that kids were being blocked from engaging in this unbridled kind of craving for social attention and dopamine responses, that could significantly address the issue. Chair DURBIN. Thank you. I'm going to recognize Senator Grassley, and then Senator Coons is going to preside as I make a dash to vote and return. So, Senator Grassley, the floor is yours.

Senator GRASSLEY. Thank you, Mr. Chairman. Thanks to all your witnesses. I'm sorry I missed your testimony for other reasons that's already been explained to you. I'm glad that we're here, discussing this very important issue today. I happen to be a father, grandfather, and great-grandfather, but regardless, we've all got to be—with this worthy cause that we're discussing today, Congress has and will continue to play a crucial role.

Unfortunately, Congress has had to intervene in times in the past. I just want to remind people of the Larry Nassar thing, dealing with young girls and the botched investigation of the FBI. And Senator Ossoff and I got a bill passed that would further give Federal intervention in the case of those crimes being committed, if they're committed outside the United States by somebody following young people to international meets.

It's also important to hold online service providers accountable in keeping our children safe. This EARN IT Act, which I was an original co-sponsor of last year, ensures online service providers that fail to crack down on certain contents are not able to escape because of Section 230 intervention. And also, protecting children online also means combating human trafficking, and Senator Feinstein and I have passed legislation in that area, as well.

Of course, it's impossible to discuss protecting children online without pointing out the unfortunate role of social media and the internet playing in drug overdose deaths among our children, and I look forward to discussing that strategy to prevent those. So, I'm going to go to Mr. Pizzuro first. Recently, an Iowa family lost their daughter because she bought a fake prescription pill from a drug dealer on Snapchat. It contained fentanyl. Her family is suing to try and hold Snapchat accountable.

One particular allegation is that Snapchat's algorithms connected their child with a drug dealer who she did not know previously, which I would find especially disturbing. So, for you, to the best of your ability, can you explain to this Committee how Snapchat's algorithms protect children against—with drug dealers?

Mr. PIZZURO. Thank you, Mr. Grassley. As far as the Snapchat and the algorithms, I'm not 100 percent sure on how Snapchat is doing it, but I could talk to the broader experience of cell phone usage as far as apps and drugs, because whether it's narcotics, whether it's child exploitation, whether it's pictures and videos, whether it's emojis, everything is done through that social media. Again, that's where children are. So, it's very easy to target them specifically in those realms. So, I think a lot of times you're going to have that. Again, whether it be fentanyl, whether it be marijuana, it doesn't matter the drug, but the scope is where I can target those individuals, and the offenders, as well as the individuals selling that, know that.

Senator GRASSLEY. You said you couldn't speak specifically to Snapchat, so I was going to ask you what social media needs to do differently to stop what's happening, but you could answer the second part of that question: what can the Government do better? Mr. PIZZURO. Well, the Government can do a lot better as far as that we're talking about today. We need a little bit more, first of all, uniformity, age identification, identity verification. There's a lot of times where the users—tomorrow, I can go get a phone and be whoever I want to be. I can get a phone, I can create an app, I can create a fake email address and then use it for whatever reasons I need to. So, from that perspective is that from the tech companies we need a little bit more from that moderation and that aspect: who's on what end of the phone?

Senator GRASSLEY. Okay. My next and last question will be to Ms. DeLaune, if I'm pronouncing your name right. Technology created these problems, and technology advances will be essential to fighting these problems in the future. So, can you tell me about the tools available today to address the online dangers to children? And what more should social media do and online platforms do to protect children?

Ms. DELAUNE. Thank you, Senator. There are various initiatives and technologies that are being used by some social media companies, certainly not all. And because of these tools, such as searching surgically for known child sexual abuse material, companies are able to surface it. There are other companies that are voluntarily choosing to look for online enticement and instances where children might be sextorted online, where offenders target them for imagery or for financial gain.

There's an important aspect of companies being transparent of what tools they're using, not only for the consumer to understand what platforms are doing, but also to share with one another what the best practices are. When everyone is speaking freely, we're able not only to see what works but also what significant gaps still exist.

Senator GRASSLEY. Thank you very much. Thank you, Mr. Chairman.

Senator GRAHAM [presiding]. Senator Coons.

Senator COONS. Thank you, and thank you to Chair Durbin and to Ranking Member Graham for both convening this hearing and for your ongoing work to find a bipartisan path forward. Ms. Bride and Ms. Lembke, thank you for your testimony today and for making clear and purposeful what we all know, which is that far too many Americans are spending time on social media and, in particular for young Americans, it can have harmful, even destructive or toxic impact.

We have limited research about exactly what the effects are of the design choices that social media platforms are making on childhood development and on children's mental health. We all know they design their platforms to hold our attention longer and longer, and we know, from your testimony and, many of us, through personal exposure, that it is not helpful, but we need to better understand why it's harmful and how it's harmful so we can craft solutions that will move us forward.

I've worked with Senators Klobuchar and Cassidy on a bipartisan bill, the Platform Accountability and Transparency Act, that would make social media companies work with independent researchers to validate and ensure that we understand how these platforms impact our children. The Surgeon General of the United States came and spent a day with us in Delaware and visited a youth center and listened to some of our youth from Delaware and some mental health professionals and public health professionals, to talk about this nationwide public health crisis.

Dr. Prinstein, you call in your testimony for greater transparency and reporting requirements for social media companies, including better data access for researchers. What kinds of questions about children's mental health would we be able to answer, with greater data access, and what data do researchers need that they don't currently have access to, and what are the barriers for their access?

Dr. PRINSTEIN. Thank you so much for your question. There are numerous barriers. We don't have the funding to be able to do the research that we need to do. We actually find that the number of academics who are pursuing a career in research on social media are recruited by social media companies themselves and offered salaries that make it very hard to compete in an academic environment.

The data that social media companies have would allow for a better exploration of exactly what it is that kids are viewing, how they're using social media, what they're seeing, how that's related to future behaviors, including what they log on, what they share, how they share that information. It would be tremendously valuable for scientists to be able to understand those questions and link it specifically to mental health. In fact, there is no such access right now, which is severely hindering our ability to work scientifically in this area.

Senator COONS. Thank you. Mr. Golin, you also call for Congress to implement transparency requirements to allow independent researchers to better understand the impact of social media on young Americans. The Platform Accountability and Transparency Act would require platforms to disclose information about how their algorithms actually operate, so that we could conduct that research in a reliable and stable way. Do you agree this would help parents ultimately to make better-informed decisions about the social media products their children consume?

Mr. GOLIN. I think transparency and researcher access is a critical piece of the equation. We shouldn't have to rely on courageous whistleblowers like Frances Haugen to understand what the companies already understand about how these technologies are impacting our children. So, I think it's incredibly important that we have transparency requirements and researcher access.

I will say, though, that we can't stop there. We need, also, at the same time, to have a duty of care for these platforms to limit their data collection and what they're doing with that data, so I wouldn't want to see a transparency be, you know, kicking the other policies down the road. We need to limit what the platforms are doing at the same time that we get a view into what they're doing. Senator COONS. I agree with you. Look, many of us have the

Senator COONS. I agree with you. Look, many of us have the strong sense, based on testimony we hear, based on our own experience as parents and community leaders, that this, as Senator Blumenthal called it, this toxic experiment on our children is going badly wrong. I look forward to joining in support of the Kids Online Safety Act, for example, but I also think we need to get underway with better funded, broader spectrum research, so we know exactly what is happening and what isn't and how we can fine-tune our responses.

Mr. Pizzuro, if I might, I appreciate your work to protect children by leading New Jersey's Internet Crimes Against Children Task Force. What were the biggest problems you faced when investigating leads generated by CyberTips, and how can Congress provide resources or improve the quality of those investigations?

Mr. PIZZURO. Well, there's a lack of uniformity. So, what would happen is that there's so many tips—so, like, New Jersey, for example, I think this year had 14,000. When I was there in 2015, it was 2,000. And the challenge is that there are tips within that that will result in a significant arrest, but the challenge is the volume. And the ESP and the providers that are actually giving us that information do not give us that information.

And if you go from a tip perspective, if I asked everyone in here who had an iPhone—we don't get any tips from Apple, right? So, that's, now, double that. So, I think those are the challenges. We need to have that better information. We need to have viability where we can actually protect witnesses.

Senator COONS. Last question, if I might. Ms. DeLaune, in your testimony, you said most sextortion offenders are located outside the U.S. You mention particularly Nigeria and Côte d'Ivoir. How could we better work with international partners and law enforcement to combat this growing problem?

Ms. DELAUNE. Thank you, Senator. Yes, the problem with sextortion—we're seeing a rapid increase of exponentially more reports now regarding children who are being targeted for money. It's aggressive. We talk to these victims, we talk to their parents on the phone, and it's heartbreaking. There has been a coordinated effort amongst law enforcement to identify where these offenders are coming from. This is an organized crime syndicate. Certainly, there are offenders all around the world. We are seeing that there's a criminal component with Nigeria and Ivory Coast in some instances.

And we're also working with the tech companies, because the tech companies—it takes all partners, here, to be able to find the solution. And sharing elements between companies—because offenders and children move from platform to platform, it's really important to be able to share that information so we can stop, intervene, make an adequate, good report that law enforcement would then be able to safeguard a child and hopefully hold an offender accountable.

Senator COONS. Thank you. Thank you all very much for your testimony.

Senator Graham.

Senator GRAHAM. Thank you. Thank you all. It's been a very, very helpful hearing. Ms. Bride, after the tragic loss of your son, you complained to certain apps that allowed bullying without naming who the person was. Is that correct?

Ms. BRIDE. Yes, Senator.

Senator GRAHAM. And what response did you get?

Ms. BRIDE. I reached out to Yolo, the anonymous app that was used to cyberbully my son. I told them what happened to my son, and I asked them to follow their policies, which required that they reveal the identity of the cyberbully. And I was ignored all four times.

Senator GRAHAM. Okay. So, you filed a lawsuit against these products. Is that correct?

Ms. BRIDE. Yes.

Senator GRAHAM. You're alleging they were unsafe?

Ms. BRIDE. Mm-hmm.

Senator GRAHAM. Mr. Prinstein. Is that right? Thank you. Prinstein?

Dr. PRINSTEIN. Yes. I believe there are a number of-

Senator GRAHAM. Wait a minute. Let me ask the question first. Dr. PRINSTEIN. Sorry.

Senator GRAHAM. Do you believe these products are unsafe, the way they're configured today, for children?

Dr. PRINSTEIN. The research is emerging, but we have a number of reasons to think that some of the features that are built into social media indeed are conferring harm directly to children.

Senator GRAHAM. Are you recommending to the Committee that these social media companies put warning labels on their products like we do with cigarettes? Dr. PRINSTEIN. I don't think that would hurt at all.

Senator GRAHAM. Okay. Back to Ms. Bride. So, you sued, and you were knocked out of court because of Section 230, right?

Ms. BRIDE. Yes.

Senator GRAHAM. Okay. So, how many of you—or, Mr. Prinstein, are you a practicing psychologist, psychiatrist?

Dr. PRINSTEIN. I'm a clinical psychologist. I'm not practicing at the moment.

Senator GRAHAM. Okay. Do you have a license?

Dr. PRINSTEIN. I do.

Senator GRAHAM. How many of you have a driver's license? [Witnesses raise hands.]

Now, that can be taken away from you if you do certain things. Are any of these social media companies licensed by the Government? The answer is no. Is it pretty clear that Section 230 prevents individual lawsuits against these social media companies? Everybody's nodding their head.

Is there any regulatory agency in America that has the power to change the behavior of these companies in a meaningful way? The answer is no. Are there any statutes on the book today that you think can address the harms you've all testified regarding? The answer is no. You can't sue them, there's no agency with the power to change their behavior, and there's no laws on the books that would stop this abusive behavior. Is that a fair summary of where we're at in 2023?

All the witnesses nodded. Do you think we can do better than that? Isn't that the reason you're here? The question is, why haven't we done better than that? Senator Blumenthal and I had a bill that got 25 votes on the Judiciary Committee. There're 25 of us. I can't think of any subject matter that would bring all 25 of us together. So, Mr. Chairman, in spite of all of our differences, let's make a pledge to these people. Ms.—how do you say your last name?

Ms. LEMBKE. Lembke.

Senator GRAHAM. Do you believe that your generation, particularly, has been let down?

Ms. LEMBKE. Yes, Senator, I do.

Senator GRAHAM. And you worry about future generations even being more harmed?

Ms. LEMBKE. Yes, sir, every day.

Senator GRAHAM. The behavior that we're talking about is driven by money. In terms of social media, the more eyes, the more money. Is that correct? So the financial incentive of the social media companies exists today to do more of this, not less?

Everybody nodded in the affirmative. Mr. Pizzuro, you said, of the platforms that sexual predators use—is Twitter one of them? Mr. Pizzuro. Yes.

Senator GRAHAM. Thank you.

Mr. PIZZURO. Yes, every platform. I don't think there's a platform that I haven't seen used.

Senator GRAHAM. Okay. So, if we did a regulatory consumer protection agency to hold these people to account, would that be a step in the right direction?

Mr. PIZZURO. I believe so, yes.

Senator GRAHAM. If we change Section 230 to allow more consumer pushback, would that be a step in the right direction?

Everybody nodded. If we pass the Online Child Protection Act and the EARN IT Act, would that be a step in the right direction?

Everybody nodded. Mr. Chairman, we know what to do. Let's just go do it.

Chair DURBIN [presiding]. Thank you, Senator Graham, and I accept the invitation. I might add that the Commerce Committee has jurisdiction on this issue, too, and I've spoken to Senator Cantwell. She shares the sentiment. Wouldn't it be amazing if Congress could do something on a bipartisan basis, and why not start here? So, let's continue with this hearing and with some resolve.

Senator Blumenthal.

Senator BLUMENTHAL. Thanks, Mr. Chairman, and I want to add, again, my thanks to Senator Graham for his partnership on the EARN IT Act. We've worked together on this measure that recognizes the excessive breadth of Section 230, and the idea of the EARN IT Act is very simple: that if any company wants to have any defense or immunity against legal action, it has to earn it. It has to earn it. That's why we named it the EARN IT Act. And it is a beginning. It's a step, not a stride. But it will mark major progress if we are able to pass this measure, and I am grateful to the Chairman for his support, Senator Grassley for his.

I'm going to embarrass myself a little bit. I began working on this problem when Big Tech was Little Tech, and NCMEC was so importantly helpful in this effort, and it has continued. So, I want to thank NCMEC for your continued support and work in this area.

And to Emma Lembke, Log Off is exactly what we need. And I'm going to go a little bit outside my lane, here, and suggest that we have you and a number of your supporters and members back here and that we do a little lobbying with you talking to my colleagues, which I think will overcome the massive number of lobbyists and lawyers that now Big Tech has. And, you know, Kristin, you have been such an eloquent and moving advocate, but like you, so have been many of the other parents. They've sat with Senator Blackburn and me, and those conversations and meetings have been some of the most really powerful moments, so I would invite you again to come back. I know that, for both of you and for others in this position, it's difficult to do, because you're reliving that pain. You are going through that loss. And so I want to thank you for your continuing effort, and I'd like to invite you back, too.

The EARN IT Act and the Kids Online Safety Act are the least we can do, the very least we can do, to help begin protecting against Big Tech. And the Chairman has suggested that maybe we'll have Big Tech come back. Frankly, I'm less interested in Big Tech's words than Big Tech's actions, because they've said again and again and again, Oh, well, we're for regulation, but just not that regulation. And if it's different regulation, Oh, well, that's not quite it, either. So, we're going to continue this work, and my thanks to everybody who is here today.

I want to ask Dr. Prinstein, because this report that the CDC came out with today talks not only about girls, and the crisis they are going through in this country, but also about LGBTQ+ young people and how they, particularly, are going through this crisis. Could you describe for the Committee how the addictive and harmful content affects them maybe more than others, either through bullying or other kinds of toxic content driven at them?

Dr. PRINSTEIN. Absolutely. Thank you. The LGBT+ community is experiencing a disproportionate amount of mental health issues, particularly related to the stress they experience as a marginalized or minoritized group. They are also experiencing a much higher rate of self-harm and suicide compared to others.

The research on social media has demonstrated a remarkably high proportion of posts that are discriminatory or hateful either to the entire LGBT+ community or to individuals based on their LGBTQ+ status. So, it's very important to recognize that online discrimination does have an effect on mental health directly. It is important, however, to recognize that the online community also provides vital health information and does provide social support that can be beneficial to this community, so it's a complex situation but one that deserves tremendous attention. Thank you.

Senator BLUMENTHAL. Thank you. Thank you to all the panel for being here today. Thanks, Mr. Chairman.

Chair DURBIN. Thank you, Senator Blumenthal.

Senator Cornyn.

Senator CORNYN. Thank you, Mr. Chairman. Thank you to the witnesses for being here today. As I've been listening to the testimony, it's just another reminder of how frustrating and maddening and, frankly, infuriating it is that Congress has been unable to deal with this in a more timely and a more targeted manner, but I'm also reminded of the fact that technology does not move at the speed of legislation, and it seems like the people who profit from this technology, these apps, are very adaptable to whatever obstacle, whatever penalty that Congress might impose. But, Mr. Pizzuro, I think it was you that made a comment. It really jumped out at me. You said, "We ought to make use of children's data illegal." Did you say that?

Mr. PIZZURO. I'm sorry, Senator. No, I didn't.

Senator CORNYN. Excuse me. Doctor-

Mr. PIZZURO. Yes.

Senator CORNYN. Doctor, you said that.

Dr. PRINSTEIN. Yes.

Senator CORNYN. Okay. And in thinking about the model, the business model of these apps, they're primarily designed to hoover up data, including personal data, and then use that data then to apply algorithms to it, to provide additional enticement or encouragement for people to continue using that app. Is that correct, Doctor?

Dr. PRINSTEIN. Yes, it is.

Senator CORNYN. And so if we were able to figure out how to make use of a minor's data illegal and had appropriate penalties, that would attack the business model and go after the people who profit from this technology, correct?

Dr. PRINSTEIN. I believe so.

Senator CORNYN. Well, maybe there's something fairly straightforward we could do in that area, because as I said, obviously legislation moves very slowly, and the people who profit and benefit from this sort of technology are very adaptable and move at a much different speed than we do.

Ms. Bride, we all grieve with you over your loss of your son, but in listening to your testimony, it seems to me that you did just about everything that a parent might do to protect your child, but yet you weren't able to completely protect him from the cyberbullying. Can you talk a little more about the role of parents in protecting their children? And are there other things that parents should do, that you weren't able to do or didn't occur to you at the time?

Ms. BRIDE. Thank you for the question, Senator. Yes, parents absolutely have a role, like we took, in talking to their kids about online safety and managing screen time, but we're at a situation right now where, if I can give you all a visual, it is like a firehose of harmful content being sprayed at our kids every day, and it's constantly changing. And I wish I could testify and say, "All you have to do as a parent is these five things and you can hand the phone over and your kid will be safe." But that would be irresponsible of me and this is why we need to go back to the source.

The source of the harm is the social media companies and their dangerous and addictive products that are designed to keep our kids online as much as possible. And in the example of anonymous apps, what better way to keep kids online but let them, in a public forum, say whatever they want to each other without their names attached?

Senator CORNYN. Dr. Prinstein, you make the point about needing more investment in mental health studies and resources. You're probably aware of this, but I'll just remind you and remind all of us that, in the Bipartisan Safer Communities Act that Congress passed last summer, we made the single largest investment in community-based mental health care in American history, together with additional resources for schools. In that context, it was in the wake of the shooting at Uvalde and the obvious failure of the mental health safety net, such as it exists, to deal with young men, in this case, who fit a dangerous profile of self-harm or harm to others.

But could you speak briefly to the workforce challenges? If we make these huge investments in mental health care, we need people to be able to provide that care, trained professionals and other associated professionals. And where are we today, in terms of providing that sort of a trained workforce to deal with the need?

Dr. PRINSTEIN. Thank you so much for the investments that you all have made so far. Unfortunately, it's just a start. The Federal Government currently funds the training of physicians at a number 750 times more than the amount that's invested in mental health professionals. The CDC report that you just saw and a number of Senators have discussed is likely a direct product of that disparity. It's critical that we are funding psychologists and other mental health providers with the same commitment and at the same level that we do our physician workforce and think about physical health.

Also, thank you for noting the importance of the slowness by which our progress is in the social media area as compared to the rapid way in which social media changes. This is also why a commitment to research on the effects of social media on mental health is so urgent now, because for us to do a study to learn how social media will affect kids over many years, it will take many years to do that study. So, we must start immediately investing much more in that research. Thank you. Chair DURBIN. Thank you, Senator Cornyn.

I'd also like to recognize the presence of former House Democratic Leader Dick Gephardt and former Lieutenant Governor Healey of Massachusetts for being here today and their work on the bipartisan Council for Responsible Social Media. Thank you for joining us.

Senator Whitehouse.

Senator WHITEHOUSE. Thank you, and let me double down on that welcome to Maura Healey for her work as attorney general, because my questions are going to be about the legal situation here. Ms. Bride, you mentioned in your testimony that your class action lawsuit was thrown out in large part because of Section 230 immunity. Is that correct?

Ms. BRIDE. Yes, that is correct.

Senator WHITEHOUSE. So, we're having kind of a bipartisan moment here today with the Blumenthal-Blackburn legislation, with the Durbin-Graham hearing, and I would be prepared to make a bet that if we took a vote on a plain Section 230 repeal, it would clear this Committee with virtually every vote. The problem, where we bog down, is that we want 230 plus. We want to repeal 230 and then have X, Y, Z, and we don't agree on what the X, Y, Z are.

I would encourage each of you, if you wish, to take a moment when the hearing is over and write down what you would like to see with respect to Section 230. If this is not your area, fine. Don't bother. Would you be happy with a flat Section 230 repeal? Would you like to see Section 230 repealed with one, two, or three other

things added? What would your recommendations be, as we look at this?

It strikes me that, when you repeal Section 230, you revert to a body of law that has stood the test of hundreds of years of experience, hundreds and thousands of trials in courtrooms around the country, and we know pretty well how to deal with it. And we've also had the experience of honest courtrooms being very important when powerful forces full of lies need to be brought to heel. And nobody knows better than Dick Blumenthal the tragedy of the families of Sandy Hook and the lies that were told about what took place that day, and it took an honest courtroom to hold the prime liar in all of that accountable.

And there was a lot of lying told about the Dominion corporation, and it took an honest courtroom—trial's still under way, discovery's still happening, but in the honest courtroom, you have the chance to dig down and see, what were the lies, and who should be held accountable, rather than just have it all be fought out in the noise of the internet and the public debate. So, to me it seems like an enormous amount of progress would be made if we would repeal Section 230. And your thoughts on that, from each of you, would be very compelling.

If there's something somebody would like to say right now, I've got 2 minutes left, and you're welcome to jump in, I mean, if you just can't hold back and you've got your answer ready. But I'd really be interested in the considered judgment of anybody who would care to answer about what the world would look like if Section 230 weren't there.

Ms. Bride?

Ms. BRIDE. Thank you, Senator. I would like to see a minimum of Section 230 repealed to the point where these companies can be held accountable for their own policies that lure kids into their products, like in the case of the anonymous apps: We monitor for cyberbullying, and we reveal the identities of those who do so. If you have that policy as a company, you need to be able to follow it, like every other industry in America.

Senator WHITEHOUSE. Yes.

Ms. BRIDE. Thank you.

Senator WHITEHOUSE. Thank you. Yes, the things we're looking at, I think, most closely here are, first, the company owns its own policies and ought to be accountable for them. That has nothing to do with something that pops up and then gets put on a platform, and when should they be accountable for what's on the platform? These are the basic operating systems designed by them, of their platform, and they should own that, period, end of story.

And the other is when they're on notice. When something is up on their platform and they know perfectly well that it's up there and they know perfectly well that it's dangerous, and they don't bother to deal with it responsibly because they know that they won't be held accountable, they can do whatever they please to try to generate clicks off even dangerous content—so, those are the areas we're looking at, and I look forward to hearing the advice from this terrific panel.

And I want to thank Chairman Durbin and Ranking Member Graham for hosting this. Senator Blackburn had stepped out and returned now. Let me just say thank you to her and to Senator Blumenthal for your terrific work together.

Chair DURBIN. Thank you, Senator Whitehouse. Senator Blackburn, you're next.

Senator BLACKBURN. Thank you, Mr. Chairman, and thank you to each of you. We are glad you're here. For everyone on the panel—and you can just give me a thumbs-up—and I am making the assumption that you all support the Kids Online Safety Act.

Okay, the record will reflect y'all are all for it. And we appreciate that. We think it is necessary. Thank you to each of you for your testimony and also for your advocacy. We appreciate this.

Ms. DeLaune, I want to come to you, if I may. The END Child Exploitation Act that I had filed last Congress, and we have this back up again—this is something that we've done because what we realize is the necessity for child exploitation to be reported to NCMEC's CyberTipline. And the bill unanimously passed through the Senate last year, and we are hopeful to get it finished. So, give me just about 30 seconds on why this bill is so important.

Ms. DELAUNE. Thank you, Senator, and thank you for your leadership on this particular Act.

Senator BLACKBURN. Sure.

Ms. DELAUNE. One of the most important components is the extension of the retention period. Many of the ESPs obviously—when they're making reports to us, the tech companies—from the moment they make the report, there is a 90-day retention notice that the companies agree to wait and hold that material if law enforcement chooses to serve legal process and gather more details.

As we've demonstrated with the exponential growth in numbers and the number of law enforcement leads that we are sending out, it is simply not enough time for law enforcement to be able to assess a report and determine whether or not an investigation must ensue. So, extending the data retention is an important part of this Act.

Senator BLACKBURN. And that was a wonderful suggestion that came to us from advocates, to extend that, because it takes longer sometimes for individuals to come forward and for law enforcement to piece that together, and the goal is to keep our children safe.

Ms. DELAUNE. Yes.

Senator BLACKBURN. So, we appreciate that. Ms. Bride, I want to come to you again. And, as always, we know how you grieve your loss, and our sympathies are with you but also our action, to get something done. Let's talk about fentanyl and the impact of fentanyl and the way children have met, whether it's on Instagram, TikTok, Snapchat, YouTube. We have worked on this issue about how these platforms need to be held accountable for the illegal activity that is taking place.

And you spoke beautifully about Carson and the bullying that was taking place with him, but we also know from other parents that you and I have met with that the introduction to drugs, the acquaintances they think are children and then they find out that they're being groomed to be pulled in to using drugs or they're being groomed to be pulled into sex trafficking. And that is one of the dangers that are there, that luring and that addiction of social media. And, Emma, you spoke so well to that, and we thank you. But let's talk a little bit about how we should be protecting children from meeting these drug dealers and pushers and traffickers online and how easy it has become for these people to impersonate children and to then ruin the lives of our children. Go ahead. I'd like for you to speak to that. I know your advocacy is in that vein.

Ms. BRIDE. Thank you, Senator. When we have met with other parents—and you've been in the room, as well—we have parents who have lost their children to fentanyl-laced drugs, and the frustration with them is they also can't get the drug dealers taken off the platform. I think I would defer to somebody else on this topic, to speak, as that's not my specific area of expertise.

Senator BLACKBURN. Yes. Ms. Bride, let me ask you this, and for any of you. For parents that have lost their kids to drug dealers, do any of you know of a drug dealer that has been apprehended, charged, indicted, convicted?

No. Isn't that amazing? It goes back to Senator Graham's point that something needs to be done about this. They're using social media as their platform.

Dr. Prinstein—oh, Mr. Chairman, my time is out. I guess I will need to yield back to you. I had one more question, so—

Chair DURBIN. Thank you, Senator.

Senator BLACKBURN. Thank you.

Chair DURBIN. Senator Hirono.

Senator HIRONO. Thank you, Mr. Chairman, and I thank all of the panelists and everyone in the audience and those who are watching these proceedings. What I get, of course, is the utter frustration that you all are sharing with us, and of course I thank my colleague for her advocacy in getting something done. Dr. Prinstein, there is a definition for addiction, and would you say that the millions of young people who are on social media—that they are exhibiting what amounts to an addiction to these platforms?

Dr. PRINSTEIN. Within the science community, we're debating over the use of that word a little bit right now, to depict social media, but I do think there's agreement that there is clearly a dependency on social media which we can see in kids suffering from many of the same symptoms that we see in the DSM, the diagnostic manual, for an addiction to substances. It seems to apply quite well to the description of kids' behavior and dependency on social media.

Senator HIRONO. And the additional danger to an addiction to social media is that this is such a negative kind of information that they can get. They're bullied, they're hassled, there are all kinds of horribly negative kinds of messages that they get from this particular addiction, which may be, you know, a little bit different. So, we do have treatments, normally, for addiction. Do we have treatments for addiction to social media?

Dr. PRINSTEIN. I don't believe those have been adequately studied.

Senator HIRONO. And we probably should study it. And that gets me to Ms. Lembke. You started on social media at sixth grade, was it? Would you say that you were addicted to social media?

Ms. LEMBKE. I will say that I exhibited—and thank you for your question, Senator—a dependency that was stated here today, but I do not think that I alone can define what that addiction means.

I think that other members of my generation and other young voices should be integrated into these ongoing conversations, into what constitutes an addiction, moving forward.

Senator HIRONO. Well, did you have a hard time not going to social media on a regular basis, on a daily basis? You spent up to 6 hours—

Ms. LEMBKE. Absolutely.

Senator HIRONO [continuing]. On these platforms? So, regardless of what the medical definition might be, that when you're spending 6 hours on a platform that didn't make you feel terribly good about yourself—so, how was it that you finally broke yourself of this dependency?

Ms. LEMBKE. Thank you, Senator, for your question. It took getting to a breaking point, where my anxiety was so great, my depression was incredibly acute, and my issues with disordered eating were rampant. It took about 3 to 4 years, getting into the ninth grade, where one day I heard the buzz of a notification, and I had the Pavlovian response to instantly grab for it, and suddenly, in that moment, I asked why. Why was I allowing these companies to have so much control over me? And that question has led to many more and has gotten me here today to speak up about the importance of having youth voices at the legislative table.

Senator HIRONO. So, I appreciate your mentioning that, your sort of, the light going off in your head—is that the kind of experience that a lot of young people who are so dependent on these platforms—that they can, of their own will, decide, I just can't take this anymore? Or is that one of the reasons that you created Log Off? Can you tell us a little bit more about what your program or the movement does to help young people?

Ms. LEMBKE. Yes, Senator. Thank you. I think each young person who struggles with this issue comes at it from a very different angle. For me, it took reaching that breaking point. For others, they continue to be harmed, and that was the reason I created Log Off. It was to seek out other young people who were frustrated, who were struggling, who were angry and wanted to talk to each other across our generation, members who understand the experience better than any other group of people across this world. So, I created that body in order to have those conversations and to work collectively to move forward in building effective solutions and in discussing those complexities in the online world and living through a digital childhood.

Senator HIRONO. Thank you very much for your stepping up. I only have a little bit of time. I want to get to Ms. Bride. There's been a lot of discussion about Section 230. A number of us have bills to reform Section 230, as do I. I think one of the concerns, though, is that the wholesale elimination of Section 230, which— I mean, I do support, you know, holding these platforms responsible for the kind of hugely harmful content, but it does get into First Amendment freedom of speech issues.

So, we need to be very aware that, as we reform Section 230 to enable, I would say, lawsuits like yours to proceed, that we do it in a careful way, to avoid unintended consequences. But I just want to share with you our deepest sympathies for what you continue to endure, and the rest of you. Thank you very much for your testimony. Thank you, Mr. Chairman.

Chair DURBIN. Thank you, Senator.

Senator Lee.

Senator LEE. Thank you, Mr. Chairman. Ms. DeLaune, I'd like to start with you, if that's all right. NCMEC does a great job of highlighting a lot of these problems and the pervasiveness of CSAM, through the CyberTipline. It's my understanding that about 32 million reports of CSAM were reported to the CyberTipline last year, and I believe you said in your testimony that, of those 32 million reports, only about 6 percent can be referred to U.S. Federal or U.S. local law enforcement here in our country. Is that right?

Ms. DELAUNE. That is correct, Senator.

Senator LEE. So, of the 32 million reports that we start with, we're already down to about 3.2 million that can be actionable here, that could be reported to law enforcement here. Would you be comfortable estimating about how many of those 32 million images of CSAM end up being removed from the internet? I think you said in your testimony somewhere that it was maybe 55 percent of those, so I'm guessing 1.7 million?

Ms. DELAUNE. We have a lot of numbers. So, for 32 million reports that are coming in the door, the reports are coming in from the tech industry, mostly, in addition to public reports. They are reporting users who are using U.S. platforms to transmit child sexual abuse material. Clearly, we have global companies here in the United States, so approximately 90 percent of the leads that are coming in are going back to other countries where offenders are uploading child sexual abuse material.

Senator LEE. Got you.

Ms. DELAUNE. So, we're down to a smaller amount of about 3.6 million reports here in the United States that we are able to refer to law enforcement. It goes to the point of—there is a lot of disparity and a long line of issues that will impact actionability of a CyberTipline report.

There are some basic key things that are necessary and are currently voluntary for tech companies to provide. That would be the images or videos or the content that meets the standard of apparent child pornography; it would be baseline information regarding the geographic location of where law enforcement should be reviewing this lead, to determine if an investigation should ensue; basic information on a user who uploaded the child sexual abuse imagery; and, if a victim existed, if they have any information. That's the baseline information that law enforcement needs.

We estimate, of the reports that we were able to provide to law enforcement last year, 55 percent of them may have been actionable, meaning they meet all of those criteria, which tells us there's a lot of improvement that can happen at the beginning of the pipeline, that quality information coming in, so law enforcement can make proper assessments.

Senator LEE. That makes a lot of sense. Now, Mr. Pizzuro, you've done some fantastic work helping kids who were in actual or imminent danger. I know that rescuing kids who are in distress should be a priority. I'm guessing that the removal of the CSAM images from the internet can't take quite as high of a priority as rescuing the kids from imminent danger. Is that the case?

Mr. PIZZURO. That's true, and one of the things is, you know, from the investigative standpoint, is those proactive cases where we're really targeting those egregious offenders.

Senator LEE. Got you. Yes, that makes sense. Look, bottom line: pornography is very bad. It's especially bad for young people. I think it's bad for everyone, but it subjects young people to significant and somewhat unique harms. It's bad enough that children were abused to make these images in the first place, but every single time these images are viewed or shared, a child's retraumatized again.

It's one of the reasons why, last year, I introduced a bill called the PROTECT Act. This is a bill that would require any websites hosting pornographic material on a commercial scale to put in place a removal mechanism and remove images at the request of the individual who appears in them. It would also require websites to verify the age of individuals appearing in pornographic material, and also they would have to verify consent. They'd be also penalized for hosting CSAM and any other items that were in there that shouldn't be, and then their victims or their authorized representatives could petition for those images to be removed from the website. And I think that would help with that.

Mr. DeLaune, in your testimony you mentioned that current law needs to be changed—Ms. DeLaune, I'm sorry—that it needs to be changed in order to help CSAM be able to share those images, help people be able to share those images with CSAM and with law enforcement. And I'd be happy to work with you on that, to get that done and to incorporate that into my bill, the PROTECT Act.

One more thing. These things are all important, and that's why, at the end of last year, I also introduced another bill called the SCREEN Act. This bill would require that any commercial website hosting pornographic images has to verify the age of users on their site and block minors from viewing graphic material. I look forward to working with my colleagues and the witnesses before us today and the organizations they represent, to get those bills across the finish line.

Finally, I just want to thank you, Ms. Bride, and you, Ms. Lembke, for sharing your stories on difficult, heart-wrenching circumstances. Thank you.

Senator OSSOFF [presiding]. Thank you, Senator Lee. I'll be managing time for a moment while Chair Durbin votes, and I'm up next, followed by Senator Kennedy. I want to thank our panel for your testimony, in particular Ms. Bride, to you, for bringing your advocacy to the Senate amidst this nightmare that you and your family have lived and continue to live. And, Ms. Lembke, thank you for your extraordinarily well considered and powerful testimony.

Ms. DeLaune, as you know and as you mentioned in your opening statement, Senator Grassley and I have legislation to strengthen Federal protections against sexual abuse of children, including online exploitation. And we were able to pass that legislation through the Senate last Congress, with bipartisan support; not yet through the House. We're hoping to do that this Congress, with your help.

And a key aspect of this bill is to ensure that the law's keeping up with technology and to ensure that when abusers use webcams or online messaging platforms to target children, that the full strength of Federal law can be brought to bear to prosecute them and to protect children from other crimes. Can you describe briefly, please, Ms. DeLaune, the necessity of ensuring that relevant Federal statutes keep up with technology and how these threats evolve?

Ms. DELAUNE. Thank you, Senator. Thank you for your leadership on that with Senator Grassley. We look forward to, you know, continuing to work with you and your staff.

It is important, as we're talking about the continual evolution of threats to our children. Technology, it was mentioned earlier, moves much faster than the legislative process, and it's very important and encouraging to be here today to hear from all of you kind of leading the charge, here, of ensuring that our legislative proposals and legislative pieces that you're considering are actually matching the technology.

What you mentioned, Senator, about live streaming that's being considered in your bill—we have seen an evolution with children being sexually exploited where there is not a physical abuser who is actually physically touching them. And we need to ensure that the legislation actually reflects that children are being exploited, children are being sexually victimized by individuals in different countries and different States and different rooms.

And this is something that we continue to see, where offenders are moving children from social media platforms, maybe where they introduce and then move them to a different platform where they would have live abuse ability, as well as individuals who are selling children for sexual performance online. So, thank you for recognizing that evolution of technology needs to be reflected in the legislation.

Senator OSSOFF. Thank you, Ms. DeLaune. And the same legislation that I've offered with Senator Grassley also strengthens law enforcement as they prosecute those who cross State lines or international lines to abuse children. What are you seeing now in terms of trends and dynamics in so-called sex tourism, particularly as it pertains to the abuse of children?

Ms. DELAUNE. Sex tourism. Certainly, you still have people who are traveling to other countries, taking advantage of lax laws and poverty to sexually exploit children. We do, of course, see now an increase—if you want to call it sex tourism, of individuals who are virtually streaming, live streaming, sexually exploiting children in impoverished countries and paying them via, you know, online apps. So, this is something that we continue to see as a problem actually getting worse because of the new ways that people can communicate live streaming.

Senator OSSOFF. Well, our bipartisan legislation, as you know, will help to crack down on online abusers, as well as those who cross State lines or international lines to attack children. I thank you for your continued support for the legislation. Finally, just briefly, Senator Blackburn ran out of time and had another question that she wanted to ask. I want to make sure to get that to Dr. Prinstein. And, Ms. Lembke, you, in a very candid and personal way, described the impact that the use of these technologies had on your psyche. And I know that, in particular for other young people around the country, they've experienced the same dynamic, the formation of dependence, the impact on selfimage and mental health. And I thank you for sharing your story.

And I want to ask you, Dr. Prinstein, if you could just speak for a moment about the long-term negative psychological impact that, in particular, young people can experience as a result of their use of social media and how we in Congress should think about addressing that.

Dr. PRINSTEIN. Scientists are working as fast as we can to give you those answers. It's something that requires us to follow kids as they mature and see how it is that they develop.

We do know that there are numerous online communities and opportunities to engage with content that actually teaches kids how to cut themselves, how to engage in behaviors that are consistent with an eating disorder, how to conceal these behaviors from their parents and adults, and they sanction young people when they discuss the possibility of engaging in an adaptive rather than maladaptive behaviors. Many of these online posts and communities have no warnings, no trigger warnings to indicate that these might be concerning for kids. And, of course, that's something that is directly associated with kids' likelihood of engaging in these maladaptive behaviors themselves.

Senator OSSOFF. Thank you, Dr. Prinstein. Deeply disturbing and certainly warrants regulatory attention. Appreciate your testimony. Senator Kennedy, you're next for 5 minutes.

Senator KENNEDY. Thank you, Senator. Many of the companies that we're talking about are American companies. Not all Big Tech is American, but we certainly led the way. These companies are very successful. They're very big, they're very powerful. They're really no longer companies—they're countries. And they're going to oppose any of this type legislation. It's why virtually nothing with respect to Big Tech has passed in the last 5 years.

I want to be fair. I think that social media has made our world smaller, which is a good thing, but it has made our world courser. And if I had to name one fault, it wouldn't be the only one, but I would say that social media has lowered the cost of being an Ahole. People say things on social media that they would never say in an interpersonal exchange. Adults, even though it's depressing sometimes, can deal with that. It's hard for young people.

We've talked about a number of problems that are presented by social media: data, privacy, sexual exploitation, but also mental health and the impact that I think it's clearly having on, particularly, young women in the Gen Z generation, 10 or 11 to 25 and 26. They're living their lives on social media, and they're not developing interpersonal relationships. It's making them very fragile. It's reaffirming this culture of victimhood. They're not getting ready for the world.

So, let me cut to the chase. I'll start with Mr.—am I saying it right? Golin?

Mr. GOLIN. Golin.

Senator KENNEDY. Golin. I apologize. For young people defined as people under the age of 16, should we just abolish social media for them, don't let them access it?

Mr. GOLIN. You know, things are so serious that I—

Senator KENNEDY. Can you give me some quick answers? Because I'm—

Mr. GOLIN. Yes.

Senator KENNEDY [continuing]. Going to go down the line.

Mr. GOLIN. We should consider all options, but I think we should focus—it makes more sense to focus on a duty of care and changing how these platforms operate. Practically, keeping kids off, under 16, may be impossible, and I would also say it's not just social media. A lot of these things happen on video game platforms, as well.

Senator KENNEDY. And you think it'll really be easy to change the attitudes of these social media companies?

Mr. GOLIN. If you create a duty of care and you limit the data that they can collect.

Senator KENNEDY. All right. I think they have a duty to care, already. What about you, Doctor?

Dr. PRINSTEIN. I think we desperately need to educate parents. Senator KENNEDY. I know we need to educate, but should we just

tell kids, "Look, it's a lot like alcohol. This stuff is addictive and until you're 16, you can't access social media"?

Dr. PRINSTEIN. There are benefits that also come from social media, and I don't know whether it's realistic to keep kids off of it completely. I think practicing moderation, with close parental supervision, with substantial education coming from the school and the home—-

Senator KENNEDY. Here's a news flash for you. A lot of parents don't care, Doctor. Mr. Pizzuro?

Mr. PIZZURO. Yes, Senator. Basically, there should be something—if I bought a phone tomorrow—there should be at least, at the very least, a terms of agreement. I can't even access that phone until I go through a 3-minute or 5-minute video.

Senator KENNEDY. Okay. Ms. DeLaune?

Ms. DELAUNE. An acknowledgment that, when you build a tool that allows adults and children to communicate with one another or find connections, that there is a duty of care to ensure that you're creating a safe environment for those kids.

Senator KENNEDY. Well, I think there's clearly a duty of care. The issue is how to enforce a duty of care. Go try to pass a bill enforcing that duty of care in the United States Congress and see what the reaction—

Ms. DELAUNE. Right.

Senator KENNEDY [continuing]. From Big Tech is.

Ms. DELAUNE. Right. Absolutely. And creating these tools, recognizing that these incidents are going to happen and finding ways that children—

Senator KENNEDY. Well, would you—

Ms. DELAUNE [continuing]. Can report them.

Senator KENNEDY [continuing]. Support a law that says, Okay, if you're under 16, you can't access social media?

Ms. DELAUNE. I think it would be difficult. There are positive things about social media, but there are many, many terrible things that kids are finding themselves in bad shape.

Senator KENNEDY. You say it would be hard. I know it'd be hard. Do you think it's a wise thing to do?

Ms. DELAUNE. I believe if the tools are designed properly, there could be benefits.

Senator KENNEDY. Okay. I can't have my—I don't have my glasses on. Yes, ma'am, your answer, please?

Ms. LEMBKE. Yes, Senator. I have not spent a lot of time thinking about specifically the right age to enter, because I do not think that it addresses the fundamental question we must answer, how to create online spaces that are safer when kids decide to enter, because I can tell you that these age restrictions—

Senator KENNEDY. Okay. Is that a no?

Ms. LEMBKE. Sorry, Senator?

Senator KENNEDY. Do you think we should prevent kids under the age of 16 from accessing social media?

Ms. LEMBKE. I think that we should spend more time looking at how to make those platforms safer, because kids will circumnavigate age restrictions.

Senator KENNEDY. Yes, ma'am.

Ms. BRIDE. And I agree with Ms. Lembke, as well. I think that safeguards is the way to go. If we look historically at the automobile industry, it was not safe, but we brought in seat belts, air bags, and now it is much safer. And we can do that with this industry.

Senator KENNEDY. Okay. Thank you.

Chair DURBIN [presiding]. Senator Klobuchar.

Senator KLOBUCHAR. Thank you very much, Mr. Chair. So, thank you so much. This has been an incredible hearing. And, as you know, I'm involved in this issue. I thank Senator Blumenthal for his work and Senator Blackburn and so many others.

So, I would agree we need rules of the road. We need rules of the road for everything from what we're talking about here for kids to privacy to competition, because there's just no rules of the road. As Senator Kennedy has expressed, we have tried in many ways and passed a number of bills in this Committee. I believe one of these days they're going to start to pass, because the social media companies have stopped everything in their tracks that we have tried to do.

And I think it is important—I guess I would start with that that they are companies, and they are media corporations, basically. And I try to explain to people that if you put something online or put it on a—one person does it, that's bad. That's one thing. Or if you yell, "Fire," in a crowded theater, okay, that's on you. But if the multiplex were to take that yelling, "Fire," and put it in all their theaters with an intercom so everyone could hear it, that's a whole nother thing. And that's a problem that hasn't been solved when it comes to these companies. They are profiting off the repeating of this information and the spreading of this information.

So, Mr. Golin, I'd just ask you this. In addition to setting the rules of the road that we want to do, when we talk about auto companies and all these other areas, at some point people have been

able to sue them for problems. And right now these companies are completely immune. Do you want to get at that and talk about your views on that?

Mr. GOLIN. Yes. I think that's a huge piece of the equation—is the ability of parents and young people themselves to hold these companies accountable. You know, Kristin talked about her lawsuit being thrown out. We work with Tawainna Anderson, whose 10year-old daughter died after attempting the viral choking challenge which TikTok put into her "For You" feed. It's not something she was searching for. TikTok's decided that this was the piece of content that would be most appealing to her at that time. And their case was thrown out of court for Section 230 reasons, as well.

Senator KLOBUCHAR. Right.

Mr. Golin. So----

Senator KLOBUCHAR. Okay. I just want to make that clear. The rules are good, but I'm telling you, if you just pretend that they are a loftier-than-any-other-company class that can't be sued for any-thing, we're never going to get a lot of these things done. So, let's be honest about that.

The Respect for Child Survivors Act is something Senator Cornyn and I passed. Mr. Prinstein, do you agree that it's important for mental health professionals to be involved in interviews of child survivors? This is this idea that whatever the crime—I was a prosecutor for quite a while—sexual abuse, whatever, it's important to have a coordinated effort when it comes to interviewing kids.

Dr. PRINSTEIN. Yes, absolutely. There's a clear psychological science around how to do that in safe and appropriate ways.

Senator KLOBUCHAR. Thank you. The issue of eating disorders— I'll go back to you, Mr. Golin. Studies have found that the eating disorders have the highest mortality rate of any mental illness. I think that surprises people. I led the Anna Westin Act, and last year, of course, thanks to Senator Blumenthal, we heard—and Senator Blackburn—from Frances Haugen, the Facebook whistleblower, about Instagram's own internal research on eating disorders. You talk about that connection between the internet and eating disorders. Do you want to quickly comment on that connection and why that should be part of our focus here?

Mr. GOLIN. Yes. So, what happens is when girls or anyone, really, expresses any interest in dieting or dissatisfaction with their body, they get barraged by content recommendations for pro-eatingdisorder content, because that's what's going to keep them engaged. So, we need to create a duty of care that these platforms have of, you know, a duty to prevent and mitigate harmful eating-disorder content and not push it on kids. I mean, I think that's one of the really important things: to distinguish between queries, where people might be interested in getting some information, versus what is being actually pushed in their feed. And frequently it is the worst, most harmful content that's being pushed in their feed.

Senator KLOBUCHAR. Okay. Ms. DeLaune, Senator Cornyn and I did a lot of work on human trafficking, as you know; passed that original bill to create incentives for safe harbor laws. Can you talk about how the internet has changed the way that human traffickers target and exploit kids? Ms. DELAUNE. Yes. Thank you, Senator. Human trafficking and child sex trafficking, in particular, has certainly been fueled by online platforms and the connectivity between offenders and children. Not only does it make buyers—it makes it easier for buyers to find children who are being trafficked, but it also allows the imagery of these children to continue to circulate, and that often keeps the victims quiet and being silenced, in terms of speaking up, because their images are then being transmitted online for potential buyers to locate.

Senator KLOBUCHAR. Okay. Last question. Mr. Pizzuro, thanks for your work. I have heard heart-wrenching stories of young people who've died after taking drugs, in one case drugs they bought on Snapchat through messages. A child named Devin suffering from dental pain bought what he thought was Percocet, and it was laced with fentanyl, and this was off of Snapchat. As his mom, Bridgette, said, "All of the hopes and dreams we as parents had for Devin were erased in the blink of an eye, and no mom should have to bury their kid." Could you talk about whether or not the social media companies are doing enough to stop the sale of drugs to kids online?

Mr. PIZZURO. The social media companies aren't doing anything, period. I think that's part of the problem, and that comes to drugs, as well. There's no moderation. Again, they're not looking at things specifically. They're not looking—again, you can't, from a communications standpoint—but that's what they're promoting, the social media, the interaction of people, so my opinion really is that we haven't seen anything, and we haven't seen any help from them.

Senator KLOBUCHAR. All right. Thank you.

Chair DURBIN. Thank you, Senator Klobuchar.

Senator Hawley.

Senator HAWLEY. Thank you, Mr. Chairman. Thanks to all of the witnesses for being here. Ms. Bride, I want to start with you. I want to particularly thank you for being willing to share your story and Carson's story. I'm the father of three, two boys, and you've lived every parent's nightmare, but thank you for being willing to try and see some good come of that and for being so bold in telling your family's story.

I want to ask you about one thing that I heard you say, and you've also written it in your written testimony, about Carson. You said, "It wasn't until Carson was a freshman in high school"—so, about 14, I would guess—"that we finally allowed him to have social media, because"—this is what caught my attention—"that was how all the students were making new connections."

Could you just say something about that? Because that's the experience, I think, of every parent. My boys are 10 and 8, and they're not on social media yet, but I know they'll want to be soon, because they'll say, "Well, everybody else is on it." So, could you just say a word about that?

Ms. BRIDE. Yes. Thank you. We waited as long as we possibly could, and we were receiving a lot of pressure from our son to be involved. And I hear this a lot from other parents. You don't want to isolate your kid, either. And so we felt, by waiting as long as possible, talking about the harms—"Don't ever send anything that you don't want on a billboard with your name and face next to it"— that we were doing all the right things and that he was old enough. He was by far the last kid in his class to get access to this technology, yet this still happened to us.

Senator HAWLEY. Yes. That's just incredible. Well, you were good parents, and you were a good mother, an incredibly good mother, clearly. This is why I supported and introduced legislation to set 16 years old as the age threshold for which kids can get on social media and require the social media companies to verify it.

I heard your answers, down the panel, a second ago, to Senator Kennedy. I just have to say this. As a father, myself, when you say things like, "Well, the parents really ought to be educated"—listen, the kids' ability—and I bet you had this experience, Ms. Bride. The kids' ability to figure out how to set what's on this phone [holding up a cell phone], my 10-year-old knows more about this phone than I know about it, already. What's it going to be like in another 4 years, or 5 or 6 years, like your son, Ms. Bride?

So, I just say, as a parent, it would put me much more in the driver's seat if the law was you couldn't have a phone—or, sorry, you couldn't get on social media until 16. I mean, that would help me, as a parent. So, that's why I'm proposing it. Parents are in favor of it. I got the idea from parents who came to me and said, "Please help us." You know, "Please help us." And listen, I'm all for tech training. It's great. But I just don't think that's going to cut it. So, I've introduced legislation to do it. Let's keep it simple. Let's put this power in the hands of parents. I'd start there.

Second thing, Ms. Bride. You brought suit against Snapchat and others. And I've got your lawsuit right here. And you were barred by Section 230, and you've testified to that effect. They just threw it all out, right?

Ms. BRIDE. Mm-hmm.

Senator HAWLEY. The court threw it all out?

Ms. BRIDE. Right. And it wasn't-

Senator HAWLEY. Go ahead.

Ms. BRIDE. The lawsuit was not about content. It was about the company's own policies—

Senator HAWLEY. Yes.

Ms. BRIDE [continuing]. That lured my son in, to think that this product, this app, was safe, this anonymous app, that they would monitor for cyberbullying and reveal the identities of those who do so. It had nothing to do with content.

Senator HAWLEY. Yes. And this is why I think it is just absolutely vital that we change the law to allow suits like yours to go forward. And if that means we have to repeal all of Section 230, I'm fine with it. I'm introducing legislation that will explicitly change Section 230 to allow suits against these social media companies for their own product design, for their own activities, for their own targeting of kids, for them to be sued for that and to allow you and every other parent, Ms. Bride, to get into Federal court.

We will create a Federal right of action, because here's what I've decided. Listen, I'm a lawyer, former attorney general. I believe in the power of courts. And what I've decided is you can fine these social media companies to death. FTC fined Facebook, what, a billion dollars or something, a couple years ago? They didn't change their behavior at all. They don't fear that. What they will fear, though, is they fear your lawsuits. That's why they fought it so hard. They don't want parents suing them. They don't want to be on the hook for damages, double damages, treble damages. Well, they should be.

And if we give the power to parents to go into court and say, "We're going to sue you," they will fear that far more than they fear some regulator here in Washington, DC, who, by the way, is probably looking to get a job with that same company when they rotate off their regulatory panel, because that's what happens. All the regulators here in DC—they go to work for these tech companies as soon as they're done here. Well, enough of that. Let's put power into the hands of parents—allow you, Ms. Bride, and every other parent in America who has a grievance here to get into court and sue these people and hold them accountable.

And I'd say the same thing about child sexual exploitation material. Let's let parents sue, and I will introduce legislation that will allow any parent in America who finds child sexual exploitation material online to go sue the companies for it. If they know or should've known, the companies, that they were hosting this material, let's let them sue them.

I tell you what, if these companies think they're going to be on the hook for multi-hundred-million-dollar-or-more fines and damages from multiple suits all across the country, they'll change their act. They'll get their act together real quick. So, my view is, enough of this complicated regulatory this, regulatory that. Just give the American people and American parents the right to get into court and defend their kids and to defend their rights. And if we do that, I think we'll see real results.

Last thing, Mr. Chairman. I know I'm going long, here, but I just want to say this. We have these hearings every so often. I love these hearings. They're great. Everybody talks tough on the companies. And then, later on, watch, we'll have votes in this Committee, real votes. And people have to put their names to stuff, and, oh, lo and behold, when that happens, we can't pass real tough stuff. So, I'd just say this to my colleagues: This has been great. Thank you, Mr. Chairman, for holding this hearing. This has been great, but it's time to vote. It's time to stand up and be counted.

I've been here for 4 years. It's been 4 years of talk. The only thing we've gotten done on Big Tech is TikTok, which we've finally banned from all Federal devices. That's the only thing of any significance we have done on Big Tech. That has got to change. And I want to thank all of you for being here, to help galvanize that change. Thanks for indulging me, Mr. Chairman.

Chair DURBIN. Thank you, Senator Hawley.

Senator Welch.

Senator WELCH. You know, this is a pretty—there's a lot of heartache in this room, and you've lived it, and I just want to acknowledge that. And what you've lived is every parent's fear. And this dilemma that we have—if there's an easy solution to it, maybe the lawsuits, as being proposed—if there was an easy solution, we'd get it. You know, I want to talk to you, Emma, just if I can. This question of whether we can have an age limit—it's appealing, but is it practical?

Ms. LEMBKE. Thank you, Senator, for your question. I have not spent a lot of time thinking through specific ages that should go on social media. I think looking at age verification is crucial in understanding how to build a productive solution, but to your point, I think the question we really have to ask is, when children, who know more than most parents, enter these online spaces, how are they protected? Because we have seen, time and time again, that no matter the bans, kids find a way in.

Senator WELCH. Right. So, they'll find a way in. And, you know, what we're hearing from you—you lost your son. The childhood sex exploitation—I mean, it's horrifying. And these are the examples of a system that has really gone amok, and it's a system that's legal. But even those kids who are not caught up and victimized in child prostitution or bullied into taking their own life—there's a mental health crisis. I mean, this is just not good for anybody. And kids— I mean, we were all kids once, and we're vulnerable at that age to what other people think of us.

So, I think there is a question here that is raised by Senator Hawley, about—how do we have responsibility at the point of entry? And that is the tech companies. And they've got a business model where they don't necessarily publish it, and of course that was Section 230, but they amplify it, as Senator Klobuchar, in her own Klobucharian way, was able to express it. And that's where the business model is sustaining this effort on the part of Big Tech, because the more clicks they get, the more advertising revenue they get.

You know, one question I have is whether it's time for us to create a governmental authority. That gets dismissed, oftentimes. But when we had previous examples like the lack of seat belts, it was the National Highway Transportation Board that was looking out after the public interest. When we had a lot of securities fraud in the 1930s, we had the Securities and Exchange Commission. It's very tough here in Congress to come up with a one-off, especially in tech, because they just keep moving ahead, and whatever we do to try to deal with the behavior of kids, they're kids, and they're going to get on that platform.

You wanted to say something, Doctor? But one of the proposals that Senator Bennet made, and I made in the House, was to have a digital authority that had some authorization from Congress. Its charge was to protect the public interest, to look at the real world about what's happening to real kids and say, "Hey, you know, this may be legal, but it ain't right, and we've got to do something." Go ahead, Doctor.

Dr. PRINSTEIN. Thank you. I appreciate your comments. I just wanted to mention an age limit is only going to be useful if there's some way to make sure that kids below that age can't get on. Remember that kids' brains are not fully matured at the age of 16. We cannot say that everything that's happening on social media now would be safe for kids at 16.

In fact, please be aware that this is the time when most kids are now starting to get autonomy, driver's licenses, and the things they're seeing online are changing the ways that they're understanding what is risky versus not. Giving kids free rein to that content just before they get in the car and drive far away from their parents might actually be short sighted.

Senator WELCH. Thank you. Ms. Bride, do you want to offer anything, after all you've been through? And thank you. I share, I think, the sentiment all of us have. It's so inspiring to see a parent try to turn tragedy into something good in the memory of her son. Thank you.

Ms. BRIDE. Thank you, Senator. I would like to see a combination of both. I would like to see Federal legislation so that these products that we know are dangerous get reviewed before they're released to American children. The example of my son, with the anonymous apps—we saw in the past they led to cyberbullying and suicides. Why were two other companies able to put out the same product?

And on the other side of it, when things go wrong, yes, I would like to see Section 230 reform so that we can hold them accountable. But it should not take grieving parents filing lawsuits to change what's happening, because it's too late for us. Thank you.

Senator WELCH. Thank you very much. I yield back, Mr. Chairman.

Chair DURBIN. Thanks, Senator Welch. Senator Blumenthal has a question.

Senator BLUMENTHAL. I have. Thanks, Mr. Chairman. I'll be very, very brief. And, again, my thanks to all the members of the panel and all of the folks who have come to attend.

I share Senator Hawley's frustration and impatience, as you may have gathered, and I feel that sense of outrage at congressional inaction. And I know, Ms. Bride, you were part of our efforts during the last session, very, very much involved, as were many of the parents who are here today and others who are perhaps watching. And my question to you and perhaps to Emma Lembke is, what did that failure to act mean to you, personally?

Ms. BRIDE. Thank you, Senator. It was extremely disappointing. There was so much momentum. I made trips, along with my fellow moms that are in the written testimony today, to Washington several times. It is so difficult to tell our stories of the very worst day of our lives, over and over and over again and then not see change. We're done with the hearings. We're done with the stories. We are looking to you all for action, and I am confident that you can all come together and do this for us and for America's children. Thank you.

Senator BLUMENTHAL. Ms. Lembke, you are part of a generation that has a right to expect more from us.

Ms. LEMBKE. Yes, Senator. You know, I got on Instagram at the age of 12, and I sit in front of you all today as a 20-year-old. But, 8 years down the line, I still see and hear of the harms that I experienced 8 years ago. And what I will say to this body is that those harms will only increase from here. The mental health crisis for young people that we are witnessing will only continue to rise. So, we cannot wait another year. We cannot wait another month, another week, or another day to begin to protect the next generation from the harms that we have witnessed and heard about today.

Senator BLUMENTHAL. Thanks, Mr. Chairman.

Chair DURBIN. Thank you, Senator Blumenthal, and thanks to the panel. I don't know if any or all of you realize what you witnessed today, but this Judiciary Committee crosses the political spectrum, not just from Democrats to Republicans but from real progressives to real conservatives. And what you heard was a unanimity of purpose, and that's rare. In fact, it's almost unheard of. And it gives me some hope.

Now, we have our own problems that have to do with this institution that I work in, in terms of when things are appropriate, how to bring them up, and how to deal with the rules of the Senate. Not an easy responsibility. A challenging responsibility. But I think the urgency of this issue is going to help propel us past some of these obstacles.

One of them is a jurisdictional issue which relates to the Senate Commerce Committee, which Senator Blumenthal can tell you has a major piece of the law that we've discussed today. And we, of course, are on the Judiciary side, the criminal side of it. We have a piece of it, as well. The question is whether there is any way to build them together. I think there is. There's certainly the will from Senator Cantwell, the Chairman of the Commerce Committee, and I've spoken to her personally.

And what I'd like to promise you is this. We're going to have a markup. Now, that doesn't sound like much, but it is a big promise. It means that we are going to come together as the Judiciary Committee and put on the table the major pieces of legislation and try to decide, as a Committee, if we can agree on common goals and common efforts to reach those goals. I think we can do this, just sensing what I heard today. And I think, as a father and grandfather, that we must do it. We must do it.

Ms. Bronstein, Ms. Bride, and others who have come here because of their passion for their children that they have lost—it makes a difference. As painful as it is, it makes a difference. And, Ms. Lembke, good luck at the Hilltop, with Washington U, but you've done a great service to our country by coming here today. And for the others, thank you for sharing this information.

Now it's our turn. We've got to get down to work and roll up our sleeves. It won't be the bill I want to write. It won't be the bill you want to write. But if it is a step forward to protect children, we're going to do it. We have to do it. We have no choice.

The hearing record's going to remain open for a week, for statements to be submitted, and you may receive some questions which I ask you to respond to promptly.

[The information appears as submissions for the record.]

I thank you all for coming today and your patience and determination to do well by our children. I thank the witnesses, and the hearing stands adjourned.

[Whereupon, at 1:36 p.m., the hearing was adjourned.]

[Additional material submitted for the record follows.]

A P P E N D I X

Additional Material Submitted for the Record

Witness List Hearing before the Senate Committee on the Judiciary

"Protecting Our Children Online"

Tuesday, February 14, 2023 Hart Senate Office Building, Room 216 10:00 a.m.

Kristin Bride Survivor Parent and Social Media Reform Advocate Portland, OR

> Emma Lembke Founder Log Off Movement Birmingham, AL

Michelle C. DeLaune President and CEO National Center for Missing & Exploited Children Alexandria, VA

> John Pizzuro CEO Raven Point Pleasant, NJ

Mitch J. Prinstein, PhD, ABPP Chief Science Officer American Psychological Association Washington, D.C.

> Josh Golin Executive Director Fairplay Boston, MA

> > (45)

Testimony of Kristin Bride United States Senate Committee on the Judiciary Hearing on Protecting Our Children Online February 14, 2023

Thank you, Chairman Durbin, Ranking Member Graham, and members of the committee. My name is Kristin Bride. I am a survivor parent and social media reform advocate, and member of the bipartisan Council for Responsible Social Media.

I am testifying here today to bring a face to the harms occurring every day resulting from the unchecked power of the social media industry. This is my son Carson Bride with beautiful blue eyes, an amazing smile, and a great sense of humor, who will be forever 16 years old. As involved parents raising our two sons in Oregon, we thought we were doing everything right. We waited until Carson was in 8th grade to give him his first cell phone, an old phone with no apps. We talked to our boys about online safety and the importance of never sending anything online that you wouldn't want your name and face next to on a billboard. Carson followed these guidelines. Yet tragedy still struck our family.

It was June 2020; Carson had just gotten his first summer job making pizzas, and after a successful first night of training, he wrote his upcoming work schedule on our kitchen calendar. We expressed how proud we were of him for finding a job during the pandemic. In so many ways, it was a wonderful night, and we were looking forward to summer. The next morning, I woke to the complete shock and horror that Carson had hung himself in our garage while we slept.

In the weeks that followed, we learned that Carson had been viciously cyberbullied by his "Snapchat friends," his high school classmates who were using the anonymous apps Yolo and LMK on Snapchat to hide their identities. It wasn't until Carson was a freshman in high school that we finally allowed him to have social media because that was how all the students were making new connections. What we didn't know is that apps like Yolo and LMK were using popular social media platforms to promote anonymous messaging to hundreds of millions of teen users.

After his death, we discovered that Carson had received nearly 100 negative, harassing, sexually explicit, and humiliating messages, including 40 in just one day. He asked his tormentors to "swipe up" and identify themselves so they could talk things out in person. No one ever did. The last search on his phone before Carson ended his life was for hacks to find out the identities of his abusers.

Anonymous apps like Whisper, Sarahah, and YikYak have a long history of enabling cyberbullying, leading to teen suicides.¹ The critical flaws in these platforms are compounded by the fact that teens do not typically report being cyberbullied. They are too fearful that their phones to which they are completely addicted will be taken away or that they will be labeled a snitch by their friends.

46

Yolo's own policies stated that they would monitor for cyberbullying and reveal the identities of those who do so. I reached out to Yolo on 4 separate occasions in the months following Carson's death, letting them know what happened to my son and asking them to follow their own policies. I was ignored all 4 times. At this point, I decided to fight back.

I filed a National Class Action Lawsuit in May 2021, against Snap Inc., Yolo, and LMK.² We believe Snap Inc. suspended Yolo and LMK from their platform because of our advocacy.

However, our complaint against Yolo and LMK for product liability design defects and fraudulent product misrepresentation was dismissed in the Central District Court of California last month, citing Section 230 immunity.³ And still, new anonymous apps like NGL and sendit are appearing on social media platforms and charging teens subscription fees to reveal the messenger or provide useless hints.

I speak before you today with the tremendous responsibility to represent the many other parents who have also lost their children to social media harms. In the audience are Rose Bronstein from Illinois who lost her son Nate and Christine McComas from Maryland who lost her daughter Grace, both to suicide after being viciously cyberbullied over social media. Our numbers continue to grow exponentially with teen deaths from dangerous online challenges fed to them on TikTok, sextortion over Facebook, fentanyl-laced drugs purchased over Snapchat, and deaths from eating disorder content over Instagram. I have included the stories of my fellow survivor parent advocates in this written testimony.

Let us be clear—these are not coincidences, accidents, or unforeseen consequences. They are the direct result of products designed to hook and monetize America's children.

It should not take grieving parents filing lawsuits on behalf of their dead children to hold this industry accountable for their dangerous and addictive product designs. Federal legislation like the Kids Online Safety Act (KOSA), which requires social media companies to have a duty of care when designing their products for America's children, is long overdue. We need our lawmakers to step up, put politics aside, and finally protect all children online.

2

Thank you for this opportunity, and I look forward to answering your questions.

Cyberbullying Frequency (2022, Pew Research Center)⁴

US Teens aged 13-17 reported:

- 46% experienced cyberbullying, with offensive name calling being the most common type of harassment
- 22% had false rumors spread about them
- 17% received explicit images they didn't ask for
- 15% report being constantly asked where they are; what they are doing or who they are with by someone other than a parent
- 10% reported receiving physical threats
- 7% reported having explicit images of them shared without their consent

Cyberbullying Impact (2018, Cyberbullying Research Center)⁵

Cyberbullying is more devastating than traditional bullying because:

- The victim may not know who is bullying them due to anonymity.
- Hurtful actions go viral which increases the audience and aggressors to limitless.
- It is easier to be cruel on-line as no social cues exist.

Cyberbullying and Suicidal Ideations (2022, JAMA Network Open Study)⁶

• Cyberbullying was the #1 cause of suicidal ideations in adolescents aged 10-13 years old based on a study of 10,414 United States adolescents.

Cyberbullying Reporting:

Reasons teens don't report cyberbullying (2021)7:

- Fear of losing their access to their technology:
 - The Pew Research Center reports that 65% of parents have taken away a teen's phone or internet privileges as punishment.⁸
- They don't want to be seen as snitch and lose even more social status.
- Ashamed for being a target

Parent Concerns (2023, Pew Research)9

• 35% of parents are worried that their kids may be bullied (2nd to Anxiety and Depression)

Citations:

¹Ian Martin, Hugely Popular NGL App Offers Teenagers Anonymity In Comments About Each other (June 29, 2022), FORBES at <u>https://www.forbes.com/sites/iainmartin/2022/06/29/hugely-popular-ngl-app-offers-teenagers-anonymity-in-comments-about-each-other/</u>

²Bride et al. v. Snap Inc., Yolo Technologies Inc., Lightspace Inc., No. 21-cv-6680 (Central District of California), ECF No. 1 (Class Action Complaint)

³Bride et al. v. Snap Inc., Yolo Technologies Inc., Lightspace Inc., No. 21-ev-6680 (Central District of California), ECF No. 142 (Order Dismissing Complaint)

⁴Vogels, E. (2022, Dec 15), Teens and Cyberbullying 2022, *Pew Research Center*, https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/

⁵Hinduja, Sameer PhD., Patchin, Justin W. PhD., Cyberbullying, identification, Prevention and Response, (2018) at <u>https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2018.pdf</u>

⁶Arnon S, Brunstein Klomek A, Visoki E, et al. (2022), Association of Cyberbullying Experiences and Perpetration With Suicidality in Early Adolescence (2022). *JAMA Network Open*. 2022;5(6):e2218746. doi:10.1001/jamanetworkopen.2022.18746

⁷ Dong, Menga, (2021, Feb 9), Why Teens Don't Report Cyberbullying at https://desis.osu.edu/seniorthesis/index.php/2021/02/09/why-teens-dont-report-cyberbullying/

⁸ Pew Research Statistics (2016, Jan 7), Parents Teens & Digital Monitoring at https://www.pewresearch.org/internet/2016/01/07/parents-teens-and-digital-monitoring/

⁹ Pew Research Statistics from Pew Research Center <u>https://www.axios.com/2023/01/29/kids-parents-mental-health-depression-anxiety</u>

Social Media Harms Parent Survivor Advocates

Tawainna Anderson, Pennsylvania

Tawainna lost her 10-year-old daughter, Nylah, last year when she tried the "Blackout Challenge" in a closet of their home. TikTok's algorithm served Nylah a video featuring the dangerous challenge on her "For You" page. Tawainna discovered her daughter's body next to her phone, and the strangulation marks on her neck suggested she desperately tried to free herself before she died.

Joann Bogard, Indiana

Joann's son Mason died at age 15 years old after he participated in a challenge he'd seen on YouTube called "the Choking Game." He was rushed to the hospital, but his parents had to make the heart wrenching decision to take him off life support and donate his organs. In the years since, Joann has reported hundreds of choking game videos to YouTube, TikTok, and other platforms but they have universally told her the videos don't violate their guidelines, despite killing hundreds of children like Mason, because they have a commercial interest in maximizing content on their platforms.

Kristin Bride, Oregon

Kristin's son, Carson was 16 years old when he died by suicide after he was viciously cyberbullied by his high school "Snapchat Friends" who were using the anonymous apps Yolo and LMK to hide their identities. Carson received over 100 humiliating, threatening and sexually explicit messages before he ended his life. The last search on his phone was for hacks to find out who was abusing him. When Kristin repeatedly contacted Yolo asking them to follow their own stated policies for monitoring and revealing the identities of those who cyberbully on their platform, she was ignored all 4 times.

Rose Bronstein, Illinois

Rose's son Nate was 15 years old when he died by suicide after he was viciously cyberbullied by over 20 high school classmates. Nate received hateful and threatening messages via iMessage. A Snapchat message was created by a classmate and reposted 7 times by others. It included threats of physical harm and death. The Snapchat quickly went viral and reached hundreds of Chicago area students. Nate also received a separate Snapchat message that read "go kill yourself".

LaQuanta Hernandez, Texas

LaQuanta's 13-year-old daughter, Jazmine, was cyberbullied for months via TikTok and Instagram on the basis of her race. The bullies sent her racist comments and photos, including photoshopping her face onto Emmett Till's body after being lynched by the KKK. Instagram took over three days to take down the posts. Jazmine was too scared to sleep in her own bed until the posts were taken down.

Tracy Kemp, Texas

Tracy's 14-year-old son Brayden was among a group of Black students who were targeted by racist cyberbullies on Instagram and Snapchat. The accounts used the school's name and logo and called on other students to take and submit pictures of Black students without their consent. She says the racist cyberbullying has drastically affected her son's mental health. The anonymity these platforms provide encourages this type of abusive and bullying behavior.

Rosemarie Maneri, New York

Shylynn was 16 years old when she was contacted by an adult via Facebook who coerced her into sending inappropriate photos of herself. Although she tried to block him, he reached out to her best friend and her best friend's mom to get back into her life. He then threatened to release her photos to her friends and family if she did not continue to send him photos and continue the relationship with him. Embarrassed, scared and not knowing what to do to make it all go away, Shylynn died from suicide at just 18 years old.

Christine McComas, Maryland

Christine's 14-year-old daughter Grace went from being a joyful, active teen to death by suicide in less than a year after malicious, death-wishing and dehumanizing cyber-abuse on Twitter. Christine screenshot the abuse and sought help from multiple public agencies including schools, police and the court system to no avail. The screenshot proof of social media abuse led to the unanimous passage of Maryland's criminal statute named Grace's Law less than a year after her death. An update to Grace's Law (2.0) was passed in 2019 to keep up with digital dangers.

Annie McGrath, Wisconsin

Annie's son Griffin died at 13 years old after he participated in an online challenge called "the Choking Game." Griffin had a YouTube channel and was trying to get more likes and comments on his videos, which may have tempted him to participate in the dangerous challenge.

Maurine Molak, Texas

David Molak died by suicide at the age of 16 after months of devastating and relentless cyberbullying by a group of students on Instagram, text, video, and GroupMe. Bullies threatened him and told him he should never go back to school. The cyberbullying left him feeling helpless and hopeless because neither he nor his parents could make it stop.

Amy Neville, Arizona

At 14, Amy's son, Alexander Neville, had his whole life ahead of him until he took a single pill that he was led to believe was oxycodone. However, it contained deadly fentanyl. Snapchat made it easy for a drug dealer to connect with him. Unfortunately, Alexander's case is not a one off situation. This happens everyday all across our country.

Erin Popolo, New Jersey

Erin's daughter, Emily Murillo, was a special education student who was bullied in person for most of her school career. During the pandemic shutdown, the bullies continued to reach out to her via Snapchat and Instagram. At 17 years old Emily lost hope that she would ever be viewed as 'normal' by her peers and died by suicide in January of 2021. The bullying continued as hackers hijacked Emily's Zoomed funeral, sending cruel messages, and posting inappropriate images on the Zoom for all of Emily's mourning family to see, until they finally had to stop the funeral.

Despina Prodromidis, New York

Despina's daughter Olivia died at 15 years old after meeting an adult stranger over Snapchat – a common problem across platforms who introduce kids to adult strangers to keep them engaged and online. This man gave her a drug which turned out to be pure fentanyl.

Neveen Radwan, California

Neveen's 15-year-old daughter, Mariam, was an avid user of several social media platforms at the time of her anorexia diagnosis. These apps constantly bombarded her with "pro-ano" (proanorexia) content. The algorithms targeted her with "skinny challenges" and manipulated content that triggered her illness to an all-time high. She then embarked on a life-threatening journey of over 2 years, in multiple hospitals, and almost dying multiple times.

Mary Rodee, New York

Mary's son, Riley, died by suicide at 15 years old. He was sextorted on Facebook by an adult who pretended to be a teenage girl and then threatened to release compromising images of Riley unless he gave them thousands of dollars. Riley, ashamed and frightened, died just six hours after the contact began. Facebook never responded when Mary and Riley's father reported the incident.

Judy Rogg, California

Judy's son, Erik Robinson, died at 12 years old after participating in the "choking challenge" that was and continues to be widely circulated on YouTube. Erik rarely used YouTube – he heard about the challenge from a friend who did, a sadly common pattern that shows even children whose parents don't allow them access to social media are vulnerable to its harms. Investigators determined that Erik died from this just the day after he learned about it. He had no idea that this could cause harm or death.

Deb Schmill, Massachusetts

Deb's daughter, Becca, died at 18 years old of fentanyl poisoning from drugs she and a friend purchased from a dealer they found on Snapchat. Becca was sexually assaulted at 15 by a boy she'd met on social media and, shortly after the assault, her peers started cyberbullying her by text and over Snapchat. Becca turned to drugs to help ease the pain and was unaware the drugs she bought over Snapchat – a massive, nearly untraceable drug market thanks to the platform's design – contained fentanyl.



53

United States Senate Committee on the Judiciary

"Protecting Our Children Online"

February 14, 2023

Testimony of Michelle DeLaune, President and CEO National Center for Missing & Exploited Children

I. <u>Background</u>

The National Center for Missing & Exploited Children (NCMEC) is a private, nonprofit organization created in response to an unthinkable tragedy. In 1981, 6-year-old Adam Walsh was with his mother, Revé, in a Florida shopping mall when he vanished without a trace. Revé and John Walsh endured 10 excruciating days searching for Adam before he was found murdered 100 miles away. The Walshes channeled their grief and came together with other child advocates to create NCMEC in 1984. Over the past 38 years, NCMEC has grown into the nation's largest and most influential child protection organization on missing and exploited children issues. Today NCMEC fulfills its congressionally designated mission to help find missing children, combat child sexual exploitation, and prevent child victimization through five main programs of work relating to: (1) missing children; (2) exploited children; (3) community outreach; (4) educational and professional resources; and (5) family support.

Over the past 25 years, NCMEC has responded as child sexual exploitation emerged on the Internet and increased exponentially in volume, severity, and complexity, and efforts to detect, report, and remove child sexual abuse material (CSAM) became more challenging. Currently, several online platforms actively engage in commendable voluntary efforts to address online child sexual exploitation. New technology has facilitated the detection of previously seen CSAM, as well as chatbased crimes, such as enticement and sextortion. However, these efforts have proven inadequate to address the immensity of the problem of online child sexual exploitation.

Today we have reached an inflection point in our efforts. It is no longer feasible to rely solely on online platforms to adopt voluntary measures, especially given their near complete immunity for activity on their sites, or to hope that they will design their platforms to avoid precipitating dangers to children from sexual exploitation, enticement, and revictimization. In the nearly three years since the Senate Judiciary Committee held a hearing on these issues soon after introduction of the EARN IT Act in 2020, no comprehensive measures to protect children from online sexual exploitation have passed Congress. If the United States is going to commit to protecting children online, legislation is our only path forward to update current laws, regulate the design of online platforms to require child

safety measures, create meaningful transparency in efforts to combat online child sexual exploitation, and provide new remedies for survivors.

II. NCMEC's Programs to Combat Online Child Sexual Exploitation

As the Internet became more accessible to the general public in the 1990s, NCMEC identified a growing trend of offenders who were using the Internet to entice and sexually exploit children and openly distribute and share images of CSAM. In response, NCMEC created two core programs to combat child sexual exploitation: (1) the CyberTipline; and (2) the Child Victim Identification Program (CVIP).

A. NCMEC's CyberTipline

1. Introduction to the CyberTipline

NCMEC created the CyberTipline in 1998 to serve as an online mechanism for members of the public and electronic service providers (ESPs) to report incidents of suspected child sexual exploitation, including: child sex trafficking;¹ online enticement of children for sexual acts; child sexual abuse material (currently referred to as child pornography under the law); child sexual molestation; child sex tourism; unsolicited obscene materials sent to children; misleading domain names; and misleading words or digital images. Each year, NCMEC receives reports relating to each of these reporting categories, but the vast majority of reports relate to child sexual abuse material (CSAM).²

NCMEC's operation of the CyberTipline is a core part of fulfilling its mission to combat online child sexual exploitation. NCMEC analysts constantly triage CyberTipline reports submitted by ESPs for two central purposes: (1) to determine a potential geographic location where a child is being harmed so the report can be made available to the appropriate law enforcement agency; and (2) to ensure that reports indicating a child is in imminent danger are prioritized for immediate action.

Most members of the public will never see CSAM. This makes it essential to understand the nature of the content reported to the CyberTipline. The images and videos that are reported are not merely sexually suggestive or older teenagers who "look young." This content depicts crime scene activity. Children – including those who are too young to call for help – are raped, abused, and exploited in this imagery. The abuse is documented in images and videos and distributed repeatedly through thousands of search engines; social media; photo-sharing, file-sharing, and email services; and gaming and messenger apps. Children are physically and sexually abused each time an image or video is made. They are revictimized every time a sexually abusive image or video in which they are

¹ CSAM is images and videos (including live-streaming) depicting the sexual abuse, rape, and exploitation of a child. CSAM is often produced and shared online for free or in exchange for other imagery. Child sex trafficking is the advertisement, solicitation, or exploitation of a child through a commercial sex act, which is defined as any sex act where something of value is given to or received by a person for sexual activity. Crimes involving the production, possession, and distribution of CSAM most CSAM does not involve the elements of child sex trafficking may in some instances involve CSAM, most CSAM does not involve the elements of child sex trafficking.

² In 2022, NCMEC received 32,059,029 CyberTipline reports, of which 99.5% related to child sexual abuse material. 2.

depicted is traded online and a new predator takes personal gratification in their anguish or uses the imagery to entice another child into sexual abuse.

Every day NCMEC bears witness to the constant flow of horrific child sexual abuse and exploitive material that floods into the CyberTipline. Since its inception 25 years ago, the CyberTipline has received more than 153 million reports containing more than 321.4 million images, videos, and other content.³ Currently, NCMEC receives an average of more than 80,000 CyberTipline reports every day. It is important to note that virtually all reports made to the CyberTipline relate to content that is being shared, stored, and distributed on the open web, not the dark web.

2. ESP Reporting to the CyberTipline

After NCMEC created the CyberTipline, Congress enacted a statute, 18 U.S.C. § 2258A, which contains a basic requirement for ESPs to submit a report to NCMEC's CyberTipline when they have actual knowledge of a violation of federal child pornography laws on their platforms.⁴ While this reporting requirement drives submission of reports to the CyberTipline, it does not require ESPs to take proactive steps to detect child sexual exploitation content, remove content after it has been reported, or submit substantive, consistent information in CyberTipline reports. The statute's current gaps and inconsistencies enable many ESPs to submit reports that are incomplete, and ultimately unactionable by law enforcement; leave children unprotected online; and subject survivors to repeated revictimization.⁵

While the total numbers of reports and reported content to the CyberTipline are immense, a majority of these reports – 90% in 2022 – related to an international offender and/or victim and were made available by NCMEC to international law enforcement. Of the remaining 10% of reports submitted in 2022, 6% related to a U.S. offender or victim and were made available to the Internet Crimes Against Children (ICAC) units or federal or local law enforcement, and 4% lacked sufficient information from the reporting ESP to determine a geographic location.⁶

³ The exponential increase in the volume of images and videos being reported to the CyberTipline has complicated maintenance and storage of this content. After careful analysis and external consultation, NCMEC has determined that cloud storage is the most secure, feasible, and cost-effective manner for continued storage of content reported to the CyberTipline. However, this cannot occur unless legislation is passed to provide the necessary limited liability to cloud provider entities to enable them to provide these narrowly defined services to NCMEC.

⁴ Members of the public also can report to the CyberTipline, but unlike ESPs they do not have immunity to report actual content. Public reports constitute a small portion of reports made to the CyberTipline. In 2022, ESPs submitted 31,802,525 CyberTipline reports, and members of the public submitted only 256,504.

⁵ After survivors have been recovered from their abusive situations, many experience recurring victimization when CSAM in which they are depicted is recirculated online – often among thousands of offenders over the course of many years. While NCMEC offers several voluntary initiatives to help ESPs curtail the recirculation of images and the revictimization of survivors, ESPs are not required to engage in efforts to combat revictimization and currently there is no civil recourse for survivors when ESPs refuse to engage in these efforts. For more information on the revictimization that survivors experience, please see NCMEC's "Be the Support: Helping Victims of Child Sexual Abuse Material: A Guide for Mental Health Professionals (https://www.missingkids.org/content/dam/missingkids/pdfs/be-the-support.pdf).

⁶ NCMEC makes reports available to more than one law enforcement agency when a report contains multiple geographic locations for a reported offender and child victim or for a sender and recipient of CSAM. Reports in which an ESP provides nothing more than a date and time of incident being reported will be made available for federal law enforcement review, even if there is no useable information and the reports do not resolve to a potential geographic location.

There are no legal requirements regarding what information an ESP must include in a CyberTipline report. As a result, many ESPs do not consistently report substantive or actionable information in their reports. In 2022, 4% of CyberTipline reports contained so little information regarding the geographic location of the reported offense, that it was not possible for NCMEC to determine where in the world that offense had occurred. NCMEC categorizes reports it receives from ESPs as "actionable" or "informational" to help prioritize CyberTipline reports for law enforcement review. An actionable report contains information regarding a suspected prior, ongoing, or planned child sexual exploitation crime. An informational report contains limited information relating to child sexual exploitation or has been designated as "viral," meaning that the image was shared online in high volumes among users for inappropriate comedic effect or moral outrage.

Of the 3,248,298 reports NCMEC made available to domestic federal, state, and local law enforcement in 2022, 43% were categorized as informational by NCMEC. Of the 892,370 reports made available to the Internet Crimes Against Children (ICAC) units, just 55% were categorized as actionable. NCMEC also categorized over 400,000 reports for the ICACs as informational due to the context of the reported incident, such as a report concerning viral imagery or no apparent child sexual exploitation nexus, or due to insufficient information provided by the reporting ESP.

CSAM reported to the CyberTipline consists of "new" and "known" imagery. New imagery generally has just been produced based on the recent sexual abuse of a child, is being seen by NCMEC for the first time, or is being newly circulated online by an offender. Known imagery has been seen before by NCMEC or law enforcement, and the child has been recovered and safeguarded from abuse but continues to suffer revictimization by the recirculation of abusive imagery in which they are depicted. All CSAM is severely damaging to children – from the initial distribution of crime scene imagery of their abuse; to the continued revictimization they suffer when imagery is redistributed, often tens of thousands of times over the years; to the use of CSAM to normalize abuse with new child victims and potential offenders. For this reason, it is essential to understand that the circulation of any image or video not only is a crime, but also has long-lasting, harmful impact on children and society.

The table below shows the growth in CyberTipline reports over the past 5 years. In addition to the enormous growth in report volume, the number of files (images, videos, and other content, including chat/messaging) reported to the CyberTipline has increased to inconceivable levels in recent years.

Year		Total Number of Files (Images, Videos, Other Content) Contained in CyberTipline Reports Submitted by ESPs ⁷
2022	32,059,029	88,377,207 (images: 55.9%) (videos: 42.7%) (other content: 1.4%)

⁷ Public reports cannot contain files (images, videos, or other content). This chart represents only ESP reports.

2021	29,397,681	84,991,735 (images: 46,99%) (videos: 52,78%) (other content: 0.23%)
2020	21,751,085	65,465,314 (images: 51.47%) (videos: 48.35%) (other content: 0.18%)
2019	16,987,361	69,171,514 (images: 40.18%) (videos: 59.67%) (other content: 0.15%)
2018	18,462,422	45,828,348 (images: 50.8%) (videos: 48,5%) (other content: 0.7%)

3. NCMEC's Hash-Sharing Initiatives

The growth in CyberTipline reports over the past 5 years as documented in the above chart is largely attributable to increased use of hashing technology⁸ by online platforms in conjunction with NCMEC's expansive voluntary hash-sharing initiatives. In addition to handling tens of millions of CyberTipline reports each year, NCMEC supports four hash-sharing initiatives to support the efforts of ESPs to detect CSAM-related content on their platforms: (1) Non-Governmental Apparent Child Pornography Hash-Sharing Initiative; (2) Exploitative Hash-Sharing Initiative; (3) Industry Hash-Sharing Initiative; and (4) Youth-Produced Imagery Hash-Sharing Initiative. ESPs may choose to voluntarily participate in one or all four of these hash-sharing initiatives.

NCMEC shares CSAM hashes compiled by NCMEC and other non-profit organizations with ESPs through the Non-Governmental Hash-Sharing Initiative. The hashes NCMEC adds to this Initiative are derived solely from images and videos reported to NCMEC's CyberTipline by ESPs.⁹ As of January 31, 2023, NCMEC has added 6,482,859 hashes to this Initiative, and other non-profits have submitted an additional 6,827,053 hashes. As of January 31, 2023, 41 ESPs are participating in this hash-sharing initiative.

NCMEC shares hashes of images and videos that may not meet the U.S. legal definition of child pornography, but are sexually exploitative, through the Exploitative Hash-Sharing Initiative. The hashes added by NCMEC to this Initiative are derived solely from images and videos reported to

⁸ A hash value can be described as a digital fingerprint of a file that can be used to uniquely identify the file. If the contents of a file are modified in any way, the value of the file's hash will change significantly. Hashing is widely used for image comparison and to identify identical imagery within large sets of images.

⁹ NCMEC utilizes a three-step process to review and validate apparent child pornography images added to the Non-Governmental Apparent Child Pornography Hash-Sharing Initiative. Each file NCMEC tags to include in this Initiative must be visually reviewed and independently and consistently tagged as "Apparent Child Sexual Abuse Material" by a NCMEC analyst, manager in NCMEC's Exploited Children Division, and senior manager in NCMEC's Exploited Children Division, After final review, approved file hashes are added by a member of NCMEC's upper management to the Initiative through a tag application interface internal to NCMEC's CyberTipline database.

NCMEC's CyberTipline by ESPs. As of January 31, 2023, NCMEC has added 314,001 hashes to this Initiative, and 15 ESPs are participating in this hash-sharing initiative.

NCMEC also supports the Industry Apparent Child Pornography Hash-Sharing Initiative, which enables ESPs to share hashes of apparent CSAM with each other. As of January 31, 2023, ESPs have added a total of 3,093,557 hashes and PhotoDNA signatures, and 37 ESPs are participating in this hash-sharing initiative.

NCMEC's most recent voluntary hash-sharing program is the Youth-Produced Imagery Hash-Sharing Initiative, which operates with NCMEC's Take It Down¹⁰ program to share hashes submitted by minors of self-produced imagery in which the minors are depicted in nude, partially nude, or sexually explicit images and videos. NCMEC launched this Initiative on December 30, 2022, and as of January 31, 2023, had added a total of 1,135 hashes. Five ESPs are participating in this hash-sharing initiative.

B. NCMEC's Child Victim Identification Program

In 2002, NCMEC created the Child Victim Identification Program (CVIP) after repeatedly seeing images of the same children in CyberTipline reviews and tracking which children had been identified by law enforcement and which children were still unidentified and potentially in abusive situations. CVIP operates with three core goals: (1) to help verify if CSAM seized by law enforcement from offenders depicts previously identified child victims; (2) to help identify and locate unidentified child victims depicted in sexually abusive images and videos; and (3) to provide recovery services and restitution support to child survivors, their families, and their private legal counsel.

U.S. federal law¹¹ does not require law enforcement to submit CSAM seized from alleged offenders to CVIP, but many law enforcement agencies choose to do so based on their agencies' practices to further efforts to identify child victims and enable them to receive notice so they can seek restitution. NCMEC's CVIP fills a unique niche in determining if seized content contains known, identified child victims or new content that should be referred for victim identification efforts. In the case of known, identified child victims, NCMEC shares distribution information on a quarterly basis with the Child Pornography Victim Assistance Program within the Department of Justice, which manages the process of notifying victims who have asked to be notified when their imagery is circulated so they can pursue restitution. As of January 31, 2022, NCMEC has reviewed over 374 million images and videos submitted to CVIP and processed information relating to more than 25,000 identified child victims.

C. Current Child Exploitation Trends and Risks for Children Online

1. Lack of ESP Mandatory Reporting of All Child Sexual Exploitation Crimes

a. <u>Issues</u>

Currently, ESPs are not required to report instances of child sex trafficking or the sexual enticement of a child to NCMEC's CyberTipline. See 18 U.S.C. § 2258A. While some companies voluntarily report these crimes, the lack of mandatory reporting results in a loss of consistent reporting and

¹⁰ https://takeitdown.ncmec.org/.

¹¹ A handful of states (e.g., Florida, Louisiana, and Montana) have laws requiring state law enforcement agencies to submit CSAM to CVIP.

reduces the incentive to develop protocols and technological tools to detect and report actionable information relating to these crimes. Most significantly, children victimized by these crimes cannot rely on a CyberTipline report to alert law enforcement to their victimization and aid in their recovery. The lack of mandatory reporting also compromises the ability of child protection professionals and service providers and legislators to accurately represent the scope of the problem and how best to develop and fund prevention measures and recovery services relating to these child sex trafficking and enticement crimes.

b. <u>Proposed Solutions</u>

The EARN IT Act, first introduced in 2020, would resolve this gap in the mandatory reporting law by adding both child sex trafficking and the enticement of children for sexual purposes to the list of child sexual exploitation crimes that ESPs must report to NCMEC's CyberTipline.¹² Passage of this legislative revision would create consistency and improvements in ESP detection and reporting of these crimes; enable law enforcement to receive increased reports relating to child victims of these crimes so they can be identified and recovered; and help ensure child victims are receiving consistent resources and support, while also providing improved metrics around the occurrence of these crimes.

Additionally, some ESPs assert differing interpretations regarding the extent to which they are legally obligated to report all user conduct regarding CSAM. NCMEC believes the statutory intent and language regarding the reporting requirement is clear as to the broad scope of CSAM-related content that ESPs are required to report when they become aware of such content on their platforms. However, in order to prevent companies from relying on an artificially narrow view that leads them to refrain from submitting reports in certain instances, legislation is needed to clarify that ESPs are required to report to the CyberTipline any information relating to CSAM that they become aware of on their platforms, in addition to apparent and imminent violations of listed child sexual exploitation crimes.

2. Disparities in ESP Detection and Reporting of Child Sexual Exploitation

a. <u>Issues</u>

The voluntary nature of the current reporting system for ESPs gives rise to vast disparities in the volume, content, and actionability of reports that ESPs submit to the CyberTipline. Many providers do not consistently report content, IP addresses, user account information, or any account information relating to a child victim when they submit a CyberTipline report. These gaps and inconsistencies lay bare the reality that even considering the millions of CyberTipline reports NCMEC receives every year, there is much we do not know about the extent of child sexual exploitation online because so many companies fail to report at all, fail to report consistently across all their platforms, and fail to report consistent, actionable information relating to child sexual exploitation incidents.

In the United States, there are thousands of companies that meet the definition of an ESP and are statutorily required to report apparent child pornography they become aware of to NCMEC. However,

¹² EARN IT Act (S. 3538, 117th Congress), Section 7(a)(1)(A)(ii).

as of January 31, 2023, only about 1,500 ESPs are registered to report to the CyberTipline,¹³ and 17% of these are international companies that have no obligation to report to the CyberTipline. In 2022, despite 1,266 U.S.-based companies being registered to report, only 236 companies actually submitted CyberTipline reports. Of the 236 reporting companies, 5 companies accounted for 93% of all the CyberTipline reports submitted: Facebook, Instagram, Google, WhatsApp,¹⁴ and Omegle. One third of the remaining companies submitted less than 10 reports each to the CyberTipline. Of note, certain international ESPs, including Yubo and MindGeek that have no legal obligation to report to the CyberTipline, regularly submit more reports relating to child sexual exploitation than many U.S.based ESPs that have a statutory obligation to report and also have significantly larger user bases.

Most ESPs that are registered with and report to the CyberTipline fail to sign up to participate in any of NCMEC's voluntary hash-sharing initiatives.¹⁵ Despite NCMEC's hash-sharing initiatives making available a total of 16,718,605 hashes that could be utilized to easily detect, remove and report known CSAM and sexually exploitative imagery depicting children, only 46 ESPs have voluntarily chosen to participate in one or more of these programs. Of these 46 ESPs, 22% have not downloaded NCMEC's hash list at all in 2023.

One of the most significant disparities in ESP reporting relates to the large number of ESPs that chronically fail to submit actionable reports. As noted above, an actionable report contains information regarding a suspected prior, ongoing, or planned child sexual exploitation crime. Generally, only actionable reports have investigative value for law enforcement. When an ESP makes a report that lacks so much information that it must be designated by NCMEC as informational, or the reported incident is so old that no current information would be available, then that report cannot be investigated by law enforcement because it lacks sufficient information relating to the offender, the child victim, or the location of the abusive incident. In 2022, just over 50% of the 32.5 million reports submitted to NCMEC's CyberTipline were informational.

b. **Proposed Solutions**

Expand ESPs' retention period for CyberTipline information beyond 90 days. There are several specific legislative solutions that could ease the vast and often debilitating disparities in ESP reporting of suspected online child sexual exploitation to NCMEC's CyberTipline. Given the volume and complexity of content reported to the CyberTipline, ESPs should be required to retain material relating to reports for a longer period of time. Currently ESPs are required to retain content they report to the CyberTipline for 90 days. This time period is no longer sufficient to accommodate the volume of reports, the flow of reports to law enforcement, the initial investigative process, and law enforcement's often time-consuming engagement with ESPs regarding search warrant returns relating to reported users' accounts. In the last Congress, both the EARN IT Act (S.3538) and the END Child Exploitation Act (S.365) contained language to expand ESPs' retention of material relating to

¹³ When NCMEC registers an ESP to report to the CyberTipline, it provides the ESP with credentials to access the secure reporting system that enables an ESP to report images, files, and other content relating to its report. ¹⁴ WhatsApp is end-to-end encrypted but is able to make CyberTipline reports based on publicly facing profile photos or

publicly-facing text and chats in which a participant reports inappropriate conduct to WhatsApp See Written Testimony, Section A.3, p.5. 8

CyberTipline reports from 90 to 180 days. NCMEC urges Congress to identify an appropriate vehicle to pass this provision in the current term.

<u>Clarify that ESPs must report to the CyberTipline all online information relating to CSAM</u>. As exploitation crimes against children have evolved, some companies have parsed their reporting requirement to exclude certain types of user activity and conduct relating to CSAM. Legislative clarity is required to ensure that ESPs unequivocally understand that they are legally required to report all conduct relating to CSAM that they become aware of on their platform to the CyberTipline. Legislation also should be introduced to require ESPs to consistently and without delay remove from their platforms all content that they report to the CyberTipline.

Explore options to utilize and better enforce penalties for failure to report to the CyberTipline. While federal law provides for penalties for companies that knowingly and willfully fail to report to the CyberTipline (18 U.S.C. § 2258A(e)), NCMEC is not aware that this provision has ever been used. NCMEC would welcome an opportunity to engage with Senate Judiciary staff on how this penalty provision could be strengthened and updated to incentivize ESPs to report substantive, actionable information on a timely and consistent basis to the CyberTipline.

Consider implementing transparency reporting for ESPs. As noted above, much is unknown regarding how ESPs are detecting and reporting content. NCMEC would welcome an opportunity to engage with Senate Judiciary staff on possibilities to implement specifically defined transparency requirements for ESPs to provide Congress and the general public with substantive information regarding ESP efforts to make their platforms safer for children. In the last Congress, the EARN IT Act contained language relating to the preparation and issuance of ESP transparency reports.¹⁶

3. The Evolution of Online Sexual Exploitation Threats to Our Children

a. <u>Issues</u>

While we struggle to address existing threats to child safety online, new threats are continuously emerging. Between 2018 and 2022, NCMEC saw a 567% increase in reports relating to the sexual enticement of a child. During the COVID pandemic, NCMEC first began seeing a distinct rise in the enticement of children, especially minor girls, for sexual imagery. In 2020, NCMEC tracked predators talking openly on the dark web about how easy it was to find children to entice during COVID. The following are just a few examples of predator comments that NCMEC tracked during this time:

- "... but with all those young girls stuck at home there must be a lot of camming going on now... hopefully some nice self-productions [will] show up ;\)"
- "how many single or divorced dads are now stuck at home with their horny daughters that can't visit their boyfriends? That must create some opportunities lol"
- "I hope there are terabytes of new content being created right now with bored dads and older b rothers stuck at home all day with their kids/siblings."

¹⁶ EARN IT Act (S. 3538, 117th Congress), Section 4(a)(3)(G).

 "Great, finally some new stuff out here. I hope that means those who are stuck at home during the COVID-19 are creating some new material with their kids?!?"

Along with an increase in enticement reports came the emergence of sextortion, a form of child sexual exploitation where a child is threatened or blackmailed by a person who says they will publicly share a nude or sexual image depicting the child unless the child provides additional sexual content, submits to sexual activity, or pays money. Sextortion is one of the most rapidly evolving online sexual exploitation crimes against children that NCMEC has ever witnessed.

Just last year, NCMEC saw another evolution in this crime with the emergence of financial sextortion. Unlike sextortion relating to imagery, the goal of financial sextortion is to extort a child for money upon threat that their nude or sexually explicit images will be shared online. While minor girls are the primary target of sextortion for imagery, teenage boys are uniquely targeted for financial sextortion. While sexual offenders drive more of the traditional online enticement and sextortion threats to children, offenders who commit financial sextortion are driven by the financial element of the crime. Most offenders involved in financial sextortion are located outside the United States, primarily in Nigeria and the Ivory Coast, and are targeting U.S. children for money.

The particular pattern and execution of these crimes pose a unique threat to children. Offenders will use fake accounts and stolen online profile photos to pose as a young female and target teenage boys to convince them to produce a nude or sexually explicit image. Almost immediately after obtaining an image, the offender will demand payment through gift cards or a peer-to-peer electronic payment system and will threaten to release the child's image if payment is not received. Financial sextortion is uniquely dangerous because the crime can occur very quickly – sometimes within minutes after a child has sent the initial image of themselves, and the outcomes can be tragic. NCMEC is aware of over a dozen instances since 2021 in which a teenage boy has taken his life as a result of being victimized by financial sextortion.¹⁷

The following example underscores how heartbreakingly fast the crime of financial sextortion can occur and how trapped and desperate the child victim can feel, often with tragic outcomes. Last year, NCMEC received a CyberTipline report from an ESP that documented the following exchange between a minor and an offender, and the offender and the minor's girlfriend:

- o 8:07pm: offender makes initial contact with the minor
- 10:07pm: minor shares sexually explicit imagery

¹⁷ Ian Cull & Stephen Ellison, Police Arrest 'Sextortion' Suspect Linked to San Jose Teen's Suicide, NBC Bay Area (2022), available at <u>https://www.nbcbayarea.com/news/local/south-bay/san-jose-police-arrest-sextortion-suspect/3109016/</u>, (last visited Feb. 9, 2023); Josh Campbell & Jason Kravarik, A 17-year-old boy died by suicide hours after being scammed. The FBI says its part of a troubling increase in 'sextortion' cases, CNN (2022), available at <u>https://www.cnn.com/2022/05/20/us/ry.an-last-suicide-sextortion-california/index.html</u> (last visited Feb. 9, 2023); Justin Dennis, Streetsboro teen who died by suicide was sextortion victim; resources to help others, Fox 8 Cleveland WJW (2022), available at <u>https://fox8.com/news/streetsboro-teen-who-died-by-suicide-was-sextortion-victim-family-says/</u> (last visited Feb. 9, 2023); Keith Benman, Remembering Riley Basford after internet blackmail pushed him to 'split second and fmadness'. NY 7 News (2021), available at https://www.wwnyty.com/20210/4/06/remembering-riley-basford-after-internet.plackmail-pushed-him-split-second-madness/ (last visited Feb. 9, 2023).

- 10:23pm: offender sends message blackmailing and threatening he will release imagery unless the minor pays money
- o 12:23am: minor expresses suicidal ideation and stops messaging
- $\circ~11:47am:$ offender writes minor's girlfriend, shares image of her boyfriend, and asks if she knows him
- 12:02pm: girlfriend responds this is her boyfriend and asks when the picture was taken
- o 12:03pm: offender says he will ruin boyfriend's life with the picture
- o 12:03pm: girlfriend responds that her boyfriend killed himself last night

It is significant to note that the ESP did not report this chat to NCMEC while this child was being sextorted or even shortly afterwards. NCMEC did not receive this report until two weeks after the child had taken his life. Unfortunately, this delay in ESP reporting to the CyberTipline is not uncommon – NCMEC has received reports concerning financial sextortion that resulted in the loss of a child's life up to two months after the incident occurred.

Financial sextortion is alarming for its rapid emergence and rapid increase in reports. In 2021, NCMEC received a total of 139 reports that it identified as related to financial sextortion. In 2022, NCMEC received more than 10,000, and in the first month of 2023, NCMEC has received more than 1,000 reports relating to financial sextortion. A majority of the financial sextortion incidents reported to NCMEC occur on just 4 platforms: Instagram, Snapchat; Facebook; and Google Hangouts. Financial sextortion has been deemed such an alarming new trend that it prompted the FBI to release an unprecedented National Public Safety Alert in December 2022.¹⁸

b. <u>Proposed Solutions</u>

Enable expanded reporting by minor victims to NCMEC. One of the most devastating aspects of sextortion and financial sextortion cases is the fact that children victimized by these crimes often feel helpless, alone, and with nowhere to turn for help. NCMEC is advocating for new ways to provide children victimized by sextortion with immediate resources to report the situation, including their images, so NCMEC can add hashes of these images to its hash-sharing initiatives with ESPs to facilitate detection, reporting, and removal of the child's images. Enabling children to report nude or sexually explicit imagery in which they are depicted to NCMEC not only accelerates disrupting the dissemination of these images by offenders, but also provides a lifeline to support children who too often feel they have nowhere to turn to for help.

In an initial effort to address this gap in reporting by minors, NCMEC launched a first of its kind program titled Take It Down in December 2022.¹⁹ This program enables children to transmit to NCMEC hashes of nude, partially nude, and sexually explicit photos and videos in which they are depicted and that they have shared or posted and now believe are being circulated online. NCMEC compiles these hashes into a list that is shared with participating companies that have agreed to use the hashes to detect, report, and remove these images if they are shared on their platforms.

¹⁸ <u>https://www.justice.gov/usao-or/pr/fbi-and-partners-issue-national-public-safety-alert-financial-sextortion-schemes.</u>
¹⁹ <u>https://takeitdown.ncmec.org/.</u>

¹¹

NCMEC considers it Take It Down program as an initial, but limited, step to providing minors victimized by sextortion with resources and support. Take It Down is limited because currently U.S. law does not permit anyone, including a minor victim or an individual who is working to help the minor victim to send actual images or videos in a report to NCMEC. Because companies use a variety of hash types, and because hashes are technically fragile and can change even when the image remains visually the same, hashes sent through the Take It Down program limit the ability of ESPs to detect, report, and remove these images. NCMEC is advocating for legislative reform to ensure that minors, and those supporting and actual imagery when reporting to NCMEC. This limited exception would provide children who are at risk with a vital lifeline not only to help get their images removed, but also to receive therapeutic support.

Expansion of education and outreach regarding sextortion is essential. In NCMEC's experience, education and outreach directed to minors who might be most vulnerable to sextortion and financial sextortion can achieve tremendous results if done consistently and conducted at scale. The recent documentary film, the Hidden Pandemic,²⁰ addresses the issue of sextortion in a factual and highly accessible manner. More multimedia, mainstream resources like this documentary are needed to educate parents/guardians and others who care for children in this age group. Additionally, children who are empowered with knowledge of how offenders may seek to victimize them through sextortion are more likely to push back and avoid victimization. We need to ensure that outreach and education regarding these issues can reach all children and be more broadly promoted and incorporated into existing education programs. By informing minors and their parents/guardians and trusted adults of the risks and harms of sextortion, we can arm them to fight back if they are approached online.

The following excerpted chat was received by NCMEC last year in a CyberTipline report and demonstrates the importance of ensuring minors understand the risks they face online and how to push back when approached by an offender. This exchange occurred over the course of just 6 minutes after the offender had offered to send nude imagery to the child:

OFFENDER:	Tell me you have a Google Chat now
CHILD VICTIM:	Yh [yeah] I'm not dumb
CHILD VICTIM:	I've seen this scam before
OFFENDER:	So I want you to download the Google Chat app so we can make naked video calls now my love
CHILD VICTIM:	You're gonna ss [screenshot] and threaten to send everything to my followers if ion pay money
CHILD VICTIM:	Some dude killed himself over this shit
CHILD VICTIM:	Yk [you know] that right?
CHILD VICTIM:	No you don't bc all you care abt is the money
CHILD VICTIM:	Get a real job

²⁰ https://sextortionfilm.com/.

Consider supporting expanded sharing of signals relating to financial sextortion among industry members, financial institutions, and NCMEC. A unique attribute of financial sextortion is that it more frequently involves cross-platform abuse, with the exchange of images and threats occurring on a social media platform, and the extortion payment being made through a third-party payment provider. As part of its clearinghouse role, NCMEC works to share information and signals of cross-platform sextortion to help communicate risks relating to particular user accounts more broadly among ESPs and payment providers. This form of data sharing helps to alert companies to sextortion occurring on their platform and enables them to work to disrupt this crime. NCMEC would welcome the opportunity to engage in discussions with Senate Judiciary staff on how signal sharing among ESPs, the financial industry, and nonprofits can be facilitated to incentivize broader sharing of information relating to sextortion risks and trends.

4. <u>Failure to Ensure Mechanisms are in Place to Identify and Recover Children from</u> <u>Victimization and Reduce Revictimization</u>

a. <u>Issues</u>

As described above, child sexual exploitation crimes against children can involve both new and known content. The creation and circulation of new content always creates exigent risk to a child and is prioritized by most ESPs, NCMEC, and law enforcement. The majority of content reported to NCMEC, however, is not new and often constitutes previously seen imagery that has been redistributed online at high rates and over the course of many years. CSAM depicting certain child victims can recirculate at disturbingly high rates as increasing numbers of offenders around the world seek out and trade a victim's imagery year after year. For some child victims, NCMEC has seen over a million images and videos collected by offenders and traded with each other for their personal gratification. For one child victim, 26% of every offender collection NCMEC has received for review contains images and videos depicting her sexual abuse. As further examples, three of the most highly distributed series of CSAM images NCMEC has worked on include the following:

- Over 1.19 million graphic sexual abuse images and videos of a female child from the ages of 2-3 years old have been seen in content seized by law enforcement from over 12,800 offenders.
- Over 1.15 million graphic sexual abuse images and videos of a female child from the ages of 5-9 years old have been seen in content seized by law enforcement from over 21,500 offenders.
- Over 985,000 graphic sexual abuse images and videos of 11 male children ranging in age from 6-10 years old have been seen in content seized by law enforcement from over 16,500 offenders.

Of the nearly 85 million images, videos, and other content reported to NCMEC by ESPs in 2021, approximately 26% of the content was visually unique. The remaining 74% of the 85 million images was duplicative of content that had been previously seen by NCMEC, which means it was content that was being redistributed online by offenders over and over again.

What is often misunderstood is the severe harm, psychological impact, and physical safety concerns that arise from the continued recirculation of CSAM. While sometimes dismissed as the circulation

of "just pictures", most members of the public are not aware of the disturbing, virulent communities of offenders that communicate online to redistribute CSAM and track, harass, and share personal information relating to child victims long after they have been recovered and safeguarded from their original physical abuse. Most also do not realize the impact on a survivor when they know that sexually abusive images and videos depicting them are circulated thousands and even hundreds of thousands of times online for years after their physical abuse has ended.

Children are revictimized in every state in the United States by the continual recirculation of their images – often among thousands of offenders for years after their initial abuse. For many of these victims, their abuse persists long after their physical recovery from their initial abuser. The case examples that follow include every state represented by a member of the Senate Judiciary Committee:

Illinois

Graphic sexually abusive images depicting a female child from ages 7-10 years old being abused by her father have been identified in content seized by law enforcement from over 9,000 offenders. The abuse originally occurred over 26-28 years ago. The child was identified and recovered from her abuse after a family member searched online for a public figure whose name matched the one offenders had associated with the child's imagery and located the images.

South Carolina

Graphic sexually abusive images depicting a 9-year-old male child being abused by an adult family member have been identified in content seized by law enforcement from over 800 offenders. The abuse originally occurred over 15 years ago.

California

Graphic sexually abusive images and videos depicting two female children from ages 5-12 years old and 16-17 years old being abused by 2 adult offenders have been identified in content seized by law enforcement from over 8,000 offenders. This abuse originally occurred 21-24 years ago. The younger child has been approached in public by strangers who recognized her from the sexually abusive material, which predators have posted to the dark web with the child's real name and photos of the child as an adult.

Iowa

Graphic sexually abusive images and videos depicting an 8-year-old female child being abused by an adult family member have been identified in content seized by law enforcement from over 10,000 offenders. The abuse originally occurred over 10 years ago. Predators on the dark web circulate the child's images with her real name and physical location with comments such as: "I think she must have liked it because she never said a word."

Rhode Island

Graphic sexually abusive images and videos depicting a 9-year-old female child being abused by her father have been identified in content seized by law enforcement from over 2,200 offenders. The abuse originally occurred 10-14 years ago.

Texas

Graphic sexually abusive images, including bondage, depicting 3 female children and 1 male child ranging in ages from 3-9 years old being abused by multiple adults, including an adult babysitter, a neighbor, and one of the child's fathers have been identified in content seized by law enforcement

from over 22,100 offenders. The abuse originally occurred 13 years ago. Predators on the dark web discuss details of the abuse and how to locate images of one of the children as an adult.

Minnesota

Graphic sexually abusive images and videos depicting a male child from ages 3-5 years old and a female child from an infant-2 years old being abused by the children's mother and neighbor have been identified in content seized by law enforcement from over 1,300 offenders. The original abuse occurred 13-14 years ago.

<u>Utah</u>

Graphic sexually abusive images and videos depicting a male child from ages 6-11 years old being abused by a family friend have been identified in content seized by law enforcement from over 5,100 offenders. The original abuse occurred 14-19 years ago. Predators on the dark web have discussed the child's real name and praised the abuser as a "loving boyfriend" to the child.

<u>Delaware</u>

Graphic sexually abusive images and videos depicting a female child from ages 4-10 years old being abused by her stepfather have been identified in content seized by law enforcement from over 5,500 offenders. This abuse originally occurred 13-18 years ago.

<u>Connecticut</u>

Graphic sexually abusive images and videos, including bondage, depicting a female child from ages 4-7 years old being abused by her guardian's partner have been identified in content seized by law enforcement from over 500 offenders. This abuse originally occurred 5-8 years ago. The child's images circulate on the dark web under the "hurtcore" category due to the physical harm and egregiousness of the abuse, and dark web commentators refer to the child as "a fussy little whore" for resisting the abuse.

<u>Missouri</u>

Graphic sexually abusive images and videos, including bondage, depicting a female child from ages 7-11 years old being abused by her guardian's partner have been identified in content seized by law enforcement from over 5,200 offenders. This abuse originally occurred 9-13 years ago. Predators on the dark web discuss the child's images and disclose her real name and physical location. They also discuss how to locate her current profiles on social media.

<u>Hawaii</u>

Graphic sexually abusive images and videos depicting 3 female children and 1 male child from ages 1-6 years old being abused by their babysitter have been identified in content seized by law enforcement from over 3,300 offenders. This abuse originally occurred 14-17 years ago.

Arkansas

Graphic sexual abuse images and videos, including bondage, depicting a female child from ages 12-14 years old being abused by her father have been identified in content seized by law enforcement from over 2,200 offenders. This abuse originally occurred 15-17 years ago.

New Jersey

Graphic sexually abusive images and videos depicting an 11-year-old female child being abused by her stepfather have been identified in content seized by law enforcement from nearly 13,000

offenders. The same offender also sexually exploited another female child in the neighborhood. This abuse originally occurred over 21 years ago.

68

<u>Louisiana</u>

Graphic sexually abusive images depicting a 10-year-old female being abused by her stepfather and mother has been identified in content seized by law enforcement from over 1,000 offenders. This abuse originally occurred 18-19 years ago.

North Carolina

Graphic sexually abusive images and videos, including bondage, depicting a 7-year-old female child being abused have been identified in content seized by law enforcement from over 16,600 offenders. This abuse originally occurred 20 years ago.

Georgia

Graphic sexually abusive images and videos, including bondage, depicting a female child from ages 5-9 years old being abused by her father have been identified in content seized by law enforcement from over 21,000 reports. This abuse originally occurred 13-15 years ago. The survivor has been tracked by offenders who have mailed packages of sex devices to her home. Predators on the dark web circulate her photos and refer to her by her real name while fantasizing that she will create an OnlyFans account or that they could rape her now.

Tennessee

Graphic sexually abusive images and videos depicting an 8-year-old male child and an infant child being abused by their adult babysitter have been identified in content seized by law enforcement from over 9,200 offenders. The original abuse occurred 8 years ago. Predators on the dark web have referred to the abuser as a "hero" and "God" and praised the videos as "just perfection."

Vermont

Graphic sexually abusive images and videos depicting an 11-year-old female child and a 9-year-old female child being abused by their father have been identified in content seized by law enforcement from collectively, 3,300 offenders. The original abuse occurred 12 years ago.

The pervasive redistribution of imagery noted in the examples above, is further exacerbated by three factors. First, there is no incentive for companies to utilize voluntary measures, such as NCMEC's hash-sharing initiatives, which have been demonstrated to greatly increase an ESP's ability to detect, remove, and report known CSAM. Even those companies that have elected to participate in these measures often do not fully engage in these initiatives.²¹

Second, there is no incentive for companies to respond to notifications from survivors or their families or lawyers or from NCMEC regarding confirmed CSAM that is posted on an ESP's platform and that needs to be removed. While many companies attempt to be responsive to such notifications, many do not or do not respond consistently or in a timely manner. An ESP's delay in removing CSAM after it has been advised of the content and its location knowingly provides for continued distribution of that imagery and causes immense harm to the survivor. NCMEC operates a notice and takedown program²² through which NCMEC will notify a company when NCMEC has received a report of

²¹ See Written Testimony, Section A.3, p.5 and Section C.2, p.8.

²² https://www.missingkids.org/content/dam/missingkids/pdfs/2021-notifications-by-ncmec-per-esp.pdf.

apparent CSAM hosted on a public website or when a survivor reaches out to NCMEC to report their imagery is posted online. In 2022, NCMEC sent more than 81,000 notices to more than 400 companies alerting them to apparent content relating to child sexual exploitation on their platforms. The companies' removal response time ranged from removing the reported content in just under 5 hours to taking over 15 days after receiving NCMEC's notice to remove the content. Some companies never responded at all to NCMEC's notice.

Third, ESPs are empowered to inaction by knowing that a victim has no available legal remedies if an ESP does not remove content when informed directly by NCMEC or a victim that CSAM is hosted on their platform. ESPs currently have immunity and therefore no legal consequences for disregarding notices from NCMEC and continuing to host the CSAM. A victim has no legal remedies, even if they have evidence that they or NCMEC have formally notified the company that it is hosting CSAM.

There also are gaps in the processes that would enable victims to know when sexually abusive imagery in which they are depicted is recirculated online or the extent to which recirculation of their imagery occurs. Federal law enforcement agencies are not required to submit imagery seized from offenders to NCMEC. This compromises victim identification and also limits the notification process to survivors, which is prompted by NCMEC's review of seized content submitted by law enforcement and conducted by the Department of Justice.²³ In addition to the lack of any requirement to submit seized content to NCMEC, the current manual process disincentives and burdens law enforcement from submitting content.²⁴ Because not all seized content is sent to NCMEC by federal and state law enforcement agencies, victims are left unaware of an unknown number of instances in which sexually exploitative content depicting them is recirculated online and shared among offenders.

Survivors also still lack feasible legal options to seek restitution from offenders who continue to recirculate their imagery online, despite the fact that Congress provided for such options when it passed the Amy, Vicky, and Andy Act (AVAA) in 2018. The AVAA created an easily accessible, consistent process for victims depicted in redistributed CSAM images to receive restitution²⁵ for the harm they suffered. Despite Congress' efforts, the AVAA has not yet been fully enacted because the Department of Justice has not issued the necessary regulations to fully establish this civil restitution program. This over 4-year delay in fully enacting remedies that Congress provided for survivors is depriving survivors of much needed restitution for therapy, medical care, continuing their education, and a small amount of financial stability during their recovery process.

Potential Solutions b.

Formalize NCMEC's notice and takedown program. NCMEC's notice and takedown program has demonstrated how a trusted flagger system can work to expedite removal of CSAM hosted on certain

 $[\]frac{^{23}}{^{24}}$ Currently law enforcement must create a physical copy of content seized from an offender and mail the content to NCMEC where it is physically uploaded into NCMEC's system for image comparison. This manual, time-consuming, and costly process disincentivizes submission of seized content to NCMEC. After careful analysis and external consultation, NCMEC has determined that utilizing electronic file transfer systems is the most secure, feasible, and costeffective manner to facilitate submission of seized content to NCMEC. However, this cannot occur unless legislation is passed to provide the necessary limited liability to electronic file transfer entities to enable them to provide these narrowly defined services to NCMEC

 $^{^{25}}$ The Amy, Vicky, and Andy Act uses the term "defined monetary assistance" to define the funds that a victim may receive under the Act.

providers. The program also has shown the need for a more robust system that not only enables victims to formally track requests to companies to remove CSAM in which they are depicted, but also provides victims with an enforcement mechanism if a company fails to remove the reported CSAM. NCMEC would welcome an opportunity to engage in discussions with Senate Judiciary staff on legislative solutions that could rely on NCMEC's existing notice and takedown program as part of a larger initiative to provide victims with a remedy when an ESP neglects or refuses to be responsive to their request to remove CSAM in which they are depicted.

Mandate submitting seized content to NCMEC and facilitate electronic submissions. When content seized from offenders is not submitted to NCMEC's CVIP, unidentified victims lose the opportunity for law enforcement intervention and identified victims lose the opportunity to be notified of the recirculation of CSAM in which they are depicted, which results in fewer opportunities to seek restitution. These gaps could be filled with 2 legislative measures: (1) a requirement that federal agencies submit all content seized from an offender to NCMEC for victim identification and to track distribution for restitution purposes; and (2) passing legislation to enable law enforcement and NCMEC to utilize electronic file transfer systems to alleviate the disincentives of the time-consuming manual process that law enforcement must currently engage in to submit seized content to NCMEC.

Direct the Department of Justice to issue AVAA regulations. Victims are still waiting to receive the full benefit of legal remedies from the AVAA that Congress passed in 2018. These remedies cannot be fully realized until the Department of Justice has issued the draft regulations to implement the AVAA and completed its regulatory process. NCMEC urges the Senate Judiciary Committee to ensure that survivors depicted in sexually exploitive images redistributed online can benefit from the AVAA provisions by directing the Department of Justice to issue the AVAA regulations, bring this regulatory process to a close, and provide survivors with the legislative relief they were promised years ago.

Provide victims with a private right of action when ESPs knowingly facilitate the distribution of CSAM in which they are depicted. As discussed above, child victims have no viable recourse when an ESP knowingly hosts or facilitates the distribution of CSAM in which they are depicted or when an ESP neglects or refuses to remove CSAM either upon a victim's request or receipt of a NCMEC notice. Victims must be provided with a basic right to seek recourse against an ESP in these circumstances. The EARN IT Act introduced in the last Congress contains a provision that would provide victims with a private right of action against ESPs that violate child pornography laws.²⁶ NCMEC urges this Committee to identify an appropriate vehicle to pass this provision in the current term. Additionally, NCMEC would welcome an opportunity to engage in discussions with Senate Judiciary staff on legislative solutions that can build on NCMEC's notice and takedown program to provide a remedy process for victims when an ESP neglects or refuses to remove CSAM after receiving a notice from NCMEC.

Update "Child Pornography" to "Child Sexual Abuse Material" in U.S. Federal statutes. Law enforcement, prosecutors, child-serving organizations, and many members of Congress have acknowledged for years that is it time to revise the term "child pornography" to "child sexual abuse material" throughout the U.S. federal statutes. The term "child pornography" is inadequate and inaccurate to describe the rape and sexual abuse of a child. The term "child sexual abuse material" more appropriately reflects that the child victim has no consent, no control, and no choice relating to

²⁶ EARN IT Act (S.3538, 117th Congress) (Section 5).

their sexual victimization or the documentation of their abuse. It is time for the United States to join many other countries around the world and call this horrific crime what it is – child sexual abuse material, not child pornography. The EARN IT Act introduced in the last Congress also contains language that would implement a complete revision of the term "child pornography" to "child sexual abuse material" throughout the U.S. federal statutes.²⁷ NCMEC urges this Committee to identify an appropriate vehicle to pass this provision in the current term.

5. <u>Failure to Ensure Online Child Safety When Adopting New Functions on Online</u> <u>Platforms</u>

a. Issues

As detailed above, we have many hurdles to overcome in addressing the current issues relating to online child sexual exploitation. We are still determining best practices and legislative measures to ensure that ESPs perform the basic functions of detecting, reporting, and removing CSAM consistently and that survivors are provided with the full extent of legal remedies. Yet the technological landscape continues to shift around us. We are on the cusp of a new era in trying to combat online child sexual exploitation as a result of significant technology developments, including the announcement by several large social media platforms that they will implement end-to-end encryption by default on user accounts and the emergence of generative AI that appears capable of creating CSAM that is visually indistinguishable from CSAM involving real children. There has never been a more opportune time to adopt a safety by design approach for new platforms and technological tools. It is essential that we work towards ensuring that online child safety risks and potential misuse of new products and platforms by offenders are evaluated before new measures are implemented or products offered to consumers.

Many online platforms increasingly utilize end-to-end encryption as a means to protect personal data in a range of online transactions, including medical and financial transactions. When end-to-end encryption is adopted by default on social media platforms and chat applications without other meaningful child safety measures being adopted, severe child safety risks arise. In an end-to-end encrypted environment, ESPs cannot use hashing technology to detect illegal activity, including online child sexual exploitation, on their platforms. Even the detection of known CSAM is not possible in an end-to-end encrypted environment. Platforms that adopt default end-to-end encryption knowingly blind themselves to online activity on their platform and render themselves incapable of detecting child sexual exploitation or securing information from their platform pursuant to lawful service of process by law enforcement in connection with any criminal investigation.

In recent months, several large ESPs that report to NCMEC have announced that they are planning and/or exploring implementing end-to-end encryption by default on their user accounts.²⁸ NCMEC's

²⁷ EARN IT Act (S.3538, 117th Congress) (Section 6).

²⁸ See, e.g. https://blog.dropbox.com/topics/company/dropbox-to-acquire-boxcryptor-assets-bring-end-to-endencryption-to-business-users (Nov. 29, 2022) (Dropbox implementing end-to-end encryption for business users); https://techcrunch.com/2022/12/02/google-is-testing-end-to-end-encryption-for-group-chats-in-the-messagesapp/?guccounter=1&guce_referer=aHR0cHM6Ly93d3cuZ29vZ2xILmNvbS8&guce_referer_sig=AQAAFLnopIIQi Fabib5f5-rOqvuz5H4tBe7U-sAXyx8F83R02aWJJ1ZMhdCZODVp_G6t99yShsuH6pLNb1WMyeNkb-hJ0oiGG6f8F _Ef886HmSTnHVNLQEZgAXetOprPF-h8uPfCeXBLAKhyUaDkNt8G6uIGhit5pirgmHcewVuS1Vb (Dec. 2, 2022) (Google testing end-to-end encryption for group chats in Messages app); https://about.fb.com/news/2023/01/expanding-

initial analysis indicates that if certain ESPs that report large numbers of CyberTipline reports move ahead with implementing default end-to-end encryption, as they have publicly committed to doing, then approximately 80% of NCMEC's reports – or over 25 million reports – could be lost. NCMEC anticipates that reports that ESPs do make after end-to-end encryption is implemented will be devoid of actionable information, rendering these reports useless to identify an offender or to help identify an endangered child and recover them from their abusive situation.

It is important to note that this anticipated loss of reports is not just an administrative function. Many reports represent a child who needs to be recovered from abuse and where intervention is needed to thwart a potential enticement or sextortion situation. The children in these reports would lose the opportunity for law enforcement to intervene, recover them from their abuse, safeguard them from further harm, and curtail their revictimization. Their abuse would continue, but ESPs that adopt end-to-end encryption would have made a choice to not detect it. This is not an acceptable outcome in any country that values its children.

b. <u>Proposed Solutions</u>

NCMEC is aware that complex technical issues and privacy interests must be weighed along with child safety in reviewing potential options to ensure a balanced solution moving forward. We also are aware that while a majority of the public may want some level of online privacy, it is unlikely they would favor an end-to-end encryption privacy solution if it means that tens of millions of child sexual exploitation incidents would be hidden, and these child victims left without help or protection from these horrific crimes. NCMEC would welcome an opportunity to engage in discussions with Senate Judiciary staff on this issue and how we can ensure that societal equities are balanced, especially when it comes to protecting children online.

III. Conclusion

NCMEC appreciates the Committee's continued dedication to addressing the horrifying increases in online CSAM and the continued emergence of new online sexual exploitation crimes directed towards children. From NCMEC's vantage point, we are approaching a crossroads in protecting children online. We need to pass certain long-discussed legislative reforms in order to prevent our society from falling behind in child protection. And we need to anticipate the complications that imminent technological changes will bring to combatting online child sexual exploitation. There are serious challenges ahead, but we are confident that with the strong leadership of the Senate Judiciary Committee we will make strides towards protecting our children online. NCMEC stands ready to address our current challenges together and to ensure that child safety online is prioritized.

features-for-end-to-end-encryption-on-messenger/ (Jan. 23, 2023) (Meta expanding default end-to-end encryption on Messenger).



Written Testimony of Josh Golin

Executive Director, Fairplay

Before the Senate Judiciary Committee

Hearing on "Protecting our Children Online"

February 14, 2023

My name is Josh Golin and I am Executive Director of Fairplay.

I would like to thank Chairman Durbin, Ranking Member Graham, and the Distinguished Members of the Committee for holding this hearing of critical importance to America's families, and for inviting me to testify.

For more than a decade, social media companies have been performing a vast uncontrolled experiment on our children. They use the reams of data they collect on young people and endless A/B testing to fine tune their platforms' algorithms and design to maximize engagement, because more time and activity on a platform means more revenue. And because the way these platforms engage with young people is largely unregulated, there is no obligation to consider and mitigate the harmful effects of their design choices on children and teens.

The resulting impact on children and families has been devastating. Compulsive overuse, exposure to harmful and age-inappropriate content, cyberbullying, eating disorders, harms to mental health, and the sexual exploitation of children are just some of the problems linked to Big Tech's insidious business model.

It doesn't have to be this way. Instead of prioritizing engagement and data collection, apps, websites, and online platforms could be built in ways that reduce risks and increase safeguards for children and teens. With many young people now spending a majority of their waking hours online and on social media, improving the digital environment so it is safer and not exploitative or addictive is one of the most important things we can do to address the mental health crisis.

But that won't happen through self-regulation. It is past time for Congress to enact legislation that expands privacy protections for young people and requires online operators to prioritize children's wellbeing in their design choices. Without meaningful congressional action, children and teens will continue to be harmed in the most serious and tragic ways by Instagram, TikTok, Snapchat, YouTube, and thousands of lesser known apps, websites, and platforms.

My testimony today will describe how many of the most serious issues facing children and teens online are a direct result of design choices made to further companies' bottom lines, and Congress's failure to enact meaningful safeguards. I will then describe the types of protections that should be included in any online safety and privacy legislation.

73

I. About Fairplay

Fairplay is the leading independent watchdog of the children's media and marketing industries. We are committed to building a world where kids can be kids, free from the false promises of marketers and the manipulations of Big Tech. Our advocacy is grounded in the overwhelming evidence that child-targeted marketing – and the excessive screen time it encourages – undermines kids' healthy development.

Through corporate campaigns and strategic regulatory filings, Fairplay and our partners have changed the child-targeted marketing and data collection practices of some of the world's biggest companies. In 2021, we led a large international coalition of parents, advocates, and child development experts to stop Meta from releasing a version of Instagram for younger children.¹ Our 2018 Federal Trade Commission complaint against Google for violating the Children's Online Privacy Protection Act (COPPA) led to the 2019 FTC settlement that required Google to pay a record fine and to limit data collection and targeted advertising on child-directed content on YouTube.² With our partners at the Center for Digital Democracy, we have filed other requests for investigation at the FTC that remain pending. We have documented, for example, that Google Play recommends apps for young children that violate COPPA and uses unfair monetization techniques;³ that TikTok has not complied with the 2019 FTC Consent Decree that it was violating COPPA;⁴ and that Prodigy, a popular online math game assigned to millions of elementary school students across the country, uses manipulative design to unfairly promote expensive subscriptions to children.⁵

Fairplay also leads the Designed with Kids in Mind Coalition, which advocates for regulations that would require operators to make the best interests of children a primary consideration

2

¹ Brett Molina and Terry Collins, *Facebook postponing Instagram for kids amid uproar from parents, lawmakers*, USA Today (Sept. 27, 2021),

https://www.usatoday.com/story/tech/2021/09/27/instagram-kids-version-app-children-pause/5881425001/. ² Campaign for a Commercial-Free Childhood (now Fairplay) and Center for Digital Democracy, *Request to Investigate Google's YouTube Online Service and Advertising Practices for Violating the Children's Online Privacy Protection Act*, Counsel for Center for Digital Democracy and Campaign for a Commercial-Free Childhood before the Federal Trade Commission (filed April 2, 2018), <u>https://fairplayforkids.org/advocates-say-googles-youtube-</u> violates-federal-childrens-privacy-law/.

³ Campaign for a Commercial-Free Childhood (now Fairplay) and Center for Digital Democracy, *Request to Investigate Google's Unfair and Deceptive Practices in Marketing Apps for Children*, Counsel for Center for Digital Democracy and Campaign for a Commercial-Free Childhood before the Federal Trade Commission (filed Dec. 12, 2018), <u>https://fairplayforkids.org/apps-which-google-rates-safe-kids-violate-their-privacy-and-expose-them-otherharms/.</u>

⁴ Campaign for a Commercial-Free Childhood (now Fairplay) and Center for Digital Democracy, *Complaint and Request for Investigation of TikTok for Violations of the Children's Online Privacy Protection Act and Implementing Rule*, Counsel for Campaign for a Commercial-Free Childhood and Center for Digital Democracy before the Federal Trade Commission (filed May 14, 2020), <u>https://fairplayforkids.org/wp-content/uploads/2020/05/tik tok complaint.pdf</u>.

⁵ Campaign for a Commercial-Free Childhood (now Fairplay), Request for Investigation of Deceptive and Unfair Practices by the Edtech Platform Prodigy, Campaign for a Commercial-Free Childhood before the Federal Trade Commission (filed Feb. 19, 2020), <u>https://fairplayforkids.org/wpcontent/uploads/2021/02/Prodigy_Complaint_Feb21.pdf</u>.

Testimony of Josh Golin, Fairplay, February 14, 2023

when designing apps, websites, and platforms likely to be accessed by young people.⁶ Fairplay and many of our coalition members actively supported the successful passage of the California Age Appropriate Design Code. We were also lead organizers on the 2022 federal legislative campaigns for the Kids Online Safety Act and the Children and Teens' Online Privacy Protection Act. And in November of last year, we filed a Petition for Rulemaking, signed by 21 organizations, urging the FTC to declare that certain design techniques used by online platforms to maximize engagement are unfair practices.⁷

Fairplay is also home to the Screen Time Action Network, a collaborative community of practitioners, educators, advocates, and parents who work to reduce excessive technology use harming children, adolescents, and families. The Action Network hosts seven work groups, including Online Harms Prevention, a group whose members include today's witness Kristin Bride and several other parents who have tragically lost their children to social media harms.

II. Children and teens spend a significant portion of their day using digital media.

Digital device use begins in early childhood: Nearly half of 2- to 4-year-olds and more than twothirds of 5- to 8-year-olds have their own tablet or smartphone.⁸ Preschool-age children average 2.5 hours of screen media use per day, and five- to eight-year-olds average about 3 hours.⁹ In a study of elementary school-aged children's digital media use during the pandemic, approximately one-third of parents reported that their children began using social media at a younger age than they had originally planned.¹⁰

Despite the fact that all major social media sites have a minimum age of 13 in their terms of service, a growing number of younger children use platforms like TikTok, Snapchat and Instagram. About half of parents of children ages 10 to 12 and 32% of parents of kids ages 7 to 9 reported their child used social media apps in the first six months of 2021.¹¹ That same year, 18% of 8- to 12-year-olds reported using social media every day, a 38% increase from just two years prior.¹² Leaked documents from TikTok revealed the company used machine learning to

⁶ Coalition members include Accountable Tech, American Academy of Pediatrics, Center for Digital Democracy, Center for Humane Technology, Children and Screens, Common Sense, Electronic Privacy Information Center, Exposure Labs: The Creators of The Social Dilemma, Fairplay, ParentsTogether, and RAINN: <u>https://designedwithkidsinmind.us/</u>.

 ⁷ Center for Digital Democracy & Fairplay, *In the Matter of Petition for Rulemaking to Prohibit the Use on Children of Design Features that Maximize for Engagement*, (filed Nov. 17 2022). <u>https://fairplayforkids.org/wp-content/uploads/2022/11/EngagementPetition.pdf</u>
 ⁸ Victoria Rideout & Michael B. Robb, *The Common Sense Census: Media Use by Kids Age Zero to Eight*, 2020,

⁸ Victoria Rideout & Michael B. Robb, The Common Sense Census: Media Use by Kids Age Zero to Eight, 2020, Common Sense Media at 25, (2020), https://www.commonsensemedia.org/sites/ default/files/research/report/2020_zero_to_eight_census_final_web.pdf.

¹⁰ Tiffany Munzer, Chioma Torres, et al., *Child Media Use During COVID-19: Associations with Contextual and Social-Emotional Factors*, 43 Journal of Developmental and Behavioral Pediatrics at 3 (2022), https://pubmed.ncbi.nlm.nih.gov/36106745/.

 ¹¹ Kristen Rogers, *Children under 10 are using social media. Parents can help them stay safe online*, CNN, (Oct. 18, 2021), <u>https://www.cnn.com/2021/10/18/health/children-social-media-apps-use-poll-wellness/index.html</u>
 ¹² Victoria Rideout, Alanna Peebles, et al., *The Common Sense Census: Media Use by Tweens and Teens* at 12, (2022), https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf.

Testimony of Josh Golin, Fairplay, February 14, 2023

analyze user accounts and classified one-third of the platform's users as under 14,¹³ which suggests platform operators are well aware that children lie about their age in order to access social media.

Further, research indicates the pandemic has increased screen media use for preteens and teenagers. In 2021, preteens (ages 8 to 12) averaged over 5.5 hours of entertainment screen time per day and teens (ages 13 to 18) averaged a remarkable 8.5 hours daily - a 17% increase from 2019 for both age groups.¹⁴ Much of this time is spent on the major social media platforms. Ninety-five percent of teens say they use YouTube, and 67% say they use TikTok.¹⁵ Thirty-five percent of teens say they are using one of the top five online platforms – YouTube, TikTok, Instagram, Snapchat, or Facebook – "almost constantly."¹⁶

Teens' and preeteens' daily screentimes vary based on race and household income. White preteens average 4.5 hours of entertainment screen time use daily, compared to Black preteens (6.5 hours) and Hispanic/Latino preteens (7 hours). White teens spend approximately 8 hours per day on screens for entertainment, while Black and Hispanic/Latino teens average approximately two hours more.¹⁷ Preteens in higher-income households spend just under 4.5 hours of screen time per day, compared to preteens in middle-income households (5.75 hours) and lower-income households (7.5 hours). Teens in higher-income households spend about 2.5 hours less daily on screens for entertainment compared to teens in lower- and middle-income households, (7 and 9.5 hours daily, respectively).¹⁸

III. Overuse of digital media is linked to a number of serious harms for young people

Increased time online and social media use is linked to serious harms for young people. As the Surgeon General has observed – and as described in detail in Section IV of this testimony – "[b]usiness models are often built around maximizing user engagement as opposed to safeguarding users' health and ensuring that users engage with one another in safe and healthy ways . . . This translates to technology companies focusing on maximizing time spent, not time well spent."¹⁹ By maximizing time and activities online, the design choices made by platforms to maximize engagement harm minors in a number of ways, including: undermining mental health, harm to body image, fostering problematic internet use, harming physical health,

¹⁸ Id.

¹³ Raymond Zhong and Sheera Frenkel, A *Third of TikTok's U.S. Users May Be 14 or Under, Raising Safety Questions,* New York Times, (Aug. 14, 2020), <u>https://www.nytimes.com/2020/08/14/technology/tiktok-underage-users-</u>ftc.html.

¹⁴ Common Sense, *The Common Sense Census: Media Use by Tweens and Teens* at 12 (2022), https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-finalweb_0.pdf.

¹⁵ Emily A. Vogels et al., *Teens, Social Media and Technology 2022*, Pew Research Center (Aug. 10, 2022), https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022.
¹⁶ Id.

¹⁷ Victoria Rideout, Alanna Peebles, et al., *The Common Sense Census: Media Use by Tweens and Teens at 12*, (2022), <u>https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf</u>.

¹⁹ Protecting Youth Mental Health: The U.S. Surgeon General's Advisory at 25 (2021),

 $[\]underline{https://www.hhs.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.gov/sites/default/files/surgeon-general-youth-mental-health-mental-health-mental-health-mental-health-mental-health-mental-h$

increasing minors' risk of contact with dangerous or harmful people, and increasing minors' exposure to age-inappropriate and otherwise harmful content.

Harm to mental health

Maximizing minors' time and activities online is linked with worse psychological wellbeing in minors in concrete and serious ways that cannot be ignored in the context of the current youth mental health crisis.

Heavy users of digital media are more likely to be unhappy, to be depressed, or to have attempted suicide.²⁰ Two nationally representative surveys of U.S. adolescents in grades 8 through 12 found "a clear pattern linking screen activities with higher levels of depressive symptoms/suicide-related outcomes and nonscreen activities with lower levels."²¹ The same research found that suicide-related outcomes became elevated after two hours or more a day of electronic device use.²² Among teens who used electronic devices five or more hours a day, a staggering 48% exhibited at least one suicide risk factor.²³ Of particular concern, a large and growing body of research indicates a strong link between time spent on social media—some of the services most relentless in their deployment of engagement-maximizing techniques—and serious mental health challenges.²⁴ More frequent and longer social media use is associated with depression,²⁵ anxiety,²⁶ and suicide risk factors.²⁷

Even if some of these documented associations are explained by children's underlying emotional challenges, the design features that online platforms deploy to maximize engagement are likely to have differential negative effects on these young people. For example, children with more negative emotionality may seek endless scrolling as a means of dissociating

²⁰ Jean M. Twenge & W. Keith Campbell, Media Use Is Linked to Lower Psychological Well-Being: Evidence from Three Datasets, 90 Psychol. Q., 311 (2019). <u>https://pubmed.ncbi.nlm.nih.gov/30859387/</u>

²¹ Jean M. Twenge et al., Increases in Depressive Symptoms, Suicide-Related Outcomes, and Suicide Rates Among U.S. Adolescents After 2010 and Links to Increased New Media Screen Time, 6 Clinical Psychol. Sci. 3, 9 (2018) https://doi.org/10.1177/2167702617723376. See also Jane Harness et al., Youth Insight About Social Media Effects on Well/III-Being and Self-Modulating Efforts, 71 J. Adolescent Health, 324-333 (Sept. 1, 2022), 10.1016/j.jadohealth.2022.04.011; Amy Orben et al., Windows of Developmental Sensitivity to Social Media, 13 Nature Comm., 1649, (2022), 10.1038/s41467-022-29296-3

²² Id. ²³ Id.

²⁴ See, e.g., K.E. Riehm et al., Associations Between Time Spent Using Social Media and Internalizing and

Externalizing Problems Among US Youth, 76 JAMA Psychiatry, 1266 (2019), https://doi.org/10.1001/jamapsychiatry.2019.2325; N. McCrae et al., Social Media and Depressive Symptoms in

Childhood and Adolescence: A Systematic Review, 2 Adolescent Res. Rev., 315 (2017), https://doi.org/10.1007/s40894-017-0053-4; H. Allcott et al., The Welfare Effects of Social Media, 110 Econ. Rev. Am. 629 (2020), https://www.aeaweb.org/articles?id=10.1257/aer.20190658

²⁵ Jean M. Twenge & W. Keith Campbell, Media Use Is Linked to Lower Psychological Well-Being: Evidence from Three Datasets, 90 Psychol. Q. at 312 (2019). <u>https://pubmed.ncbi.nlm.nih.gov/30859387/</u>

 ²⁶ Royal Society for Public Health, *#StatusOfMind: Social Media and Young People's Mental Health and Wellbeing* 8 (May 2017), <u>https://www.rsph.org.uk/static/uploaded/d125b27c-0b62-41c5-a2c0155a8887cd01.pdf</u>
 ²⁷ Jean M. Twenge & W. Keith Campbell, *Media Use Is Linked to Lower Psychological Well-Being: Evidence from Three Datasets*, 90 Psychol. Q. (2019). <u>https://pubmed.ncbi.nlm.nih.gov/30859387/</u>

Testimony of Josh Golin, Fairplay, February 14, 2023

from emotional distress,²⁸ yet may be recommended more negative content based on their previous behavior.²⁹ Former Meta employee Frances Haugen has described how the company (then called Facebook) documented this harmful cycle in its own internal research on Instagram: "And what's super tragic is Facebook's own research says, as these young women begin to consume this -- this eating disorder content, they get more and more depressed. And it actually makes them use the app more. And so, they end up in this feedback cycle where they hate their bodies more and more."³⁰

Harm to body image

Design features that maximize time spent on social media can also lead to heightened exposure to content which increases minors' susceptibility to poor body image and, consequently, disordered eating. A 2019 study of 7th and 8th graders in the *International Journal of Eating Disorders* "suggest[ed] that [social media], particularly platforms with a strong focus on image posting and viewing, is associated with elevated [disordered eating] cognitions and behaviors in young adolescents."³¹ Another study found a positive correlation between higher Instagram use and orthorexia nervosa diagnoses.³² Personal stories from sufferers of disordered eating have highlighted the link to social media,³³ as has Meta's own internal research; the documents Frances Haugen shared with the *Wall Street Journal* in 2021 revealed that Facebook has been aware at least since 2019 that "[w]e make body image issues worse for one in three teen girls."³⁴

Risk of problematic internet use and its associated harms

Maximizing time and activities online also fosters "problematic internet use"—psychologists' term for excessive internet activity that exhibits addiction, impulsivity, or compulsion.³⁵ A 2016

³³ See, e.g., Jennifer Neda John, Instagram Triggered My Eating Disorder, Slate (Oct. 14, 2021),

https://slate.com/technology/2021/10/instagram-social-media-eating-disorder-trigger.html; Clea Skopeliti, 'I Felt My Body Wasn't Good Enough': Teenage Troubles with Instagram, The Guardian (Sep. 18, 2021),

https://www.theguardian.com/society/2021/sep/18/i-felt-my-body-wasnt-good-enough-teenage-troubles-with-instagram.

³⁴ Georgia Wells et al., *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, W.S.J. (Sept. 14, 2021), https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.

³⁵ Chloe Wilkinson et al., *Screen Time: The Effects on Children's Emotional, Social, and Cognitive Development,* Informed Futures, at 6, (2021), https://informedfutures.org/wp-content/uploads/Screen-time-The-effects-onchildrens-emotional-social-cognitive-development.pdf.

²⁸Amanda Baughan et al., "I Don't Even Remember What I Read": How Design Influences Dissociation on Social Media, CHI Conference on Human Factors in Computing Systems, 1-13 (2022), https://dl.acm.org/doi/pdf/10.1145/3491102.3501899.

 ²⁹ Kait Sanchez, Go Watch this WSJ investigation of TikTok's Algorithm, The Verge, (July 21, 2021), https://www.theverge.com/2021/7/21/22587113/tiktok-algorithm-wsj-investigation-rabbit-hole.
 ³⁰ Scott Pelley, Whistleblower: Facebook is misleading the public on progress against hate speech, violence,

misinformation ,CBS, (Oct. 3, 2021), <u>https://www.cbsnews.com/news/facebook-whistleblower-frances-haugenmisinformation-public-60-minutes-2021-10-03/.</u>

³¹ Simon M. Wilksch et al., *The Relationship Between Social Media Use and Disordered Eating in Young Adolescents*, 53 Int. J. Eat. Disord. 96, 104 (2020).

³² Pixie G. Turner & Carmen E. Lefevre, *Instagram Use Is Linked to Increased Symptoms of Orthorexia Nervosa*, 22 Eating Weight Disorders 277, 281 (2017).

nationwide survey of minors ages 12 to 18 found that 61% of teens thought they spent too much time on their mobile devices, and 50% felt "addicted" to them.³⁶ In a 2022 Pew Research survey, 35% of teens said they are on YouTube, TikTok, Instagram, Snapchat, or Facebook "almost constantly."³⁷ And a report released last week by Amnesty International on young people ages 13-24 found "a staggering 74% of respondents report checking their social media accounts more than they would like to. Respondents bemoaned the 'addictive' lure of the constant stream of updates and personalized recommendations, often feeling 'overstimulated' and 'distracted."³⁸

Problematic internet use, in turn, is linked to a host of additional problems. For example, one study of 564 children between the ages of 7 and 15 found that problematic internet use was positively associated with depressive disorders, Attention Deficit Hyperactivity Disorder, general impairment, and increased sleep disturbances.³⁹ A meta-analysis of peer-reviewed studies involving cognitive findings associated with problematic internet use in both adults and adolescents found "firm evidence that [problematic internet use]. . . is associated with cognitive impairments in motor inhibitory control, working memory, Stroop attentional inhibition and decision-making."⁴⁰ Another study of over 11,000 European adolescents found that among teens exhibiting problematic internet use, 33.5% reported moderate to severe depression; 22.2% reported self-injurious behaviors such as cutting; and 42.3% reported suicidal ideation.⁴¹ The rate of attempted suicides was a staggering ten times higher for teens exhibiting problematic internet use than their peers who exhibited healthy internet use.⁴²

Harm to physical health

Maximizing minors' time spent online at the expense of sleep or movement also harms their physical health. When minors are driven to spend more time online, they sleep less for a variety of reasons – because it is impossible to be online and sleep at the same time, because stimulation before bedtime disrupts sleep patterns, and because many of the design features used by online platforms make users feel pressured to be connected constantly, and that feeling often doesn't go away at bedtime. Research shows that minors who exhibit problematic

https://www.amnesty.org/en/latest/news/2023/02/children-young-people-social-media-survey-2/. ³⁹ Restrepo et al., Problematic Internet Use in Children and Adolescents: Associations with Psychiatric Disorders and

destructive behaviours, 23 Eur. Child & Adolescent Psychiatry 1093, 1096 (2014), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4229646/. ⁴² Id.

³⁶ Common Sense, *Dealing with Devices: Parents*, 10-11, (2016), <u>https://www.commonsensemedia.org/sites/default/files/research/report/commonsense_dealingwithdevices-topline_release.pdf</u>.

 ³⁷ Emily A. Vogels et al., *Teens, Social Media and Technology 2022*, Pew Research Center (Aug. 10, 2022), https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022.
 ³⁸Amnesty International, "We are totally exposed": Young people share concerns about social media's impact on privacy and mental health in global survey (Feb. 7, 2023)

Impairment, 20 BMC Psychiatry 252 (2020), https://doi.org/10.1186/s12888-020-02640-x. ⁴⁰ Konstantinos Ioannidis et al., *Cognitive Deficits in Problematic Internet Use: Meta-Analysis of 40 Studies*, 215

British Journal of Psychiatry 639, 645 (2019), https://pubmed.ncbi.nlm.nih.gov/30784392/. ⁴¹ Michael Kaess et al., *Pathological Internet use among European adolescents: psychopathology and self-*

internet use often suffer from sleep problems.⁴³ One-third of teens report waking up and checking their phones for something other than the time at least once per night.⁴⁴ Some teens set alarms in the middle of the night to remind them to check their notifications or complete video game tasks that are only available for a limited time.⁴⁵

These behaviors in turn create new risks for young people. Screen time before bed is associated with lower academic performance.⁴⁶ Teenagers who use social media for more than five hours per day are about 70% more likely to stay up late on school nights.⁴⁷ A lack of sleep in teenagers has been linked to inability to concentrate, poor grades, drowsy-driving incidents, anxiety, depression, thoughts of suicide, and even suicide attempts.⁴⁸

A large body of research demonstrates that more time online displaces physical activity⁴⁹ and is consistently correlated with minors' risk of obesity, which in turn increases their risk of serious illnesses like diabetes, high blood pressure, heart disease, and depression.⁵⁰ Further, when minors spend more time online, they are exposed to more advertisements for unhealthy food and beverages, ⁵¹ which are heavily targeted toward minors⁵² and disproportionately marketed to Black and Hispanic youth.⁵³ In addition, poor sleep quality —which, as discussed above, is associated with problematic internet use—increases the risk of childhood obesity by 20%.54

https://pubmed.ncbi.nlm.nih.gov/22158265/.

⁴³ Anita Restrepo, Tohar Scheininger, et al., Problematic Internet Use in Children and Adolescents: Associations with Psychiatric Disorders and Impairment, 20 BMC Psychiatry 252 (2020), https://doi.org/10.1186/s12888-020-02640-

⁴⁴ Common Sense, Screens and Sleep: The New Normal: Parents, Teens, Screens, and Sleep in the United States at 7 (2019), https://www.commonsensemedia.org/sites/default/files/research/

report/2019-new-normal-parents-teens-screens-and-sleep-united-states-report.pdf.

⁴⁵ Emily Weinstein & Carrie James, Behind Their Screens: What Teens Are Facing (And Adults Are Missing), MIT Press, at 38 (2022).

⁴⁶ Chloe Wilkinson et al., Screen Time: The Effects on Children's Emotional, Social, and Cognitive Development at 4 (2021), https://informedfutures.org/wp-content/uploads/Screen-time-The-effects-on-childrens-emotional-socialcognitive-development.pdf.

⁴⁷ Heavy Social Media Use Linked to Poor Sleep, BBC News (Oct. 23, 2019), https://www.bbc.com/ news/health-50140111.

⁴⁸ Among teens, sleep deprivation an epidemic, Stanford News Ctr. (Oct. 8, 2015),

https://med.stanford.edu/news/all-news/2015/10/among-teens-sleep-deprivation-an-epidemic.html.

⁴⁹ E de Jong et al., Association Between TV Viewing, Computer Use and Overweight, Determinants and Competing Activities of Screen Time in 4- to 13-Year-Old Children, 37 Int'l J. Obesity 47, 52 (2013),

⁵⁰ Jeff Chester, Kathryn C. Montgomery, et al., Big Food, Big Tech, and the Global Childhood Obesity Pandemic at 3 (2021), https://www.democraticmedia.org/sites/default/files/field/public-files/2021/full report.pdf. ⁵¹ Id.

⁵² Jeff Chester, Kathryn C. Montgomery, et al., Big Food, Big Tech, and the Global Childhood Obesity Pandemic at 3 (2021), https://www.democraticmedia.org/sites/default/files/field/public-files/2021/full_report.pdf.

⁵³ University of Connecticut Rudd Center for Food Policy & Health et. al., *Targeted Food and Beverage Advertising* to Black and Hispanic Consumers: 2022 Update, (Nov. 2022), https://uconnruddcenter.org/wp-

content/uploads/sites/2909/2022/11/TargetedMarketing/2022-Executive-Summary.pdf. 54 Yanhui Wu et al., Short Sleep Duration and Obesity Among Children: A Systematic Review and Meta-Analysis of Prospective Studies, 11 Obesity Rsch. & Clinical Prac. 140, 148 (2015),

https://pubmed.ncbi.nlm.nih.gov/27269366/; Michelle A. Miller et al., Sleep Duration and Incidence of Obesity in Infants, Children, and Adolescents: A Systematic Review and Meta-Analysis of Prospective Studies, 41 Sleep 1, 15 (2018), https://pubmed.ncbi.nlm.nih.gov/29401314/.

Harms to Safety

The pressure to spend more time on digital media platforms and maximize interactions with other users also puts children at risk of predation. Twenty-five percent of 9-to-17-year-olds report having had an online sexually explicit interaction with someone they believed to be an adult.⁵⁵ In 2020, 17% of minors – including 14% of 9-12-year-olds – reported having shared a nude photo or video of themselves online. Of these children and teens, 50% reported having shared a nude photo or video with someone they had not met in real life, and 41% reported sharing with someone over the age of 18.⁵⁶

Design features that maximize engagement also increase young people's risk of cyberbullying. A 2022 survey by the Pew Research Center found that nearly 50% of teens reported being cyberbullied.⁵⁷ Sexual minority and gender expansive youth report being exposed to anonymous forms of cyberbullying more than their heterosexual and cisgender counterparts.⁵⁸ Cyberbullying is linked to increased risky behaviors such as smoking and increased risk of suicidal ideation.⁵⁹

It's worth noting that these serious threats to children's safety aren't limited to social media. The FTC's recent settlement with Epic Games documented how the default text and voice chat settings on Fortnite led children and teens to communicate with strangers, including adults. As a result, children were subject to harassment, bullying, and predation while playing the wildly popular game.⁶⁰

IV. The platforms where children spend the majority of their time online are designed to maximize engagement, often at the expense of children's wellbeing and safety.

Digital platforms are designed to maximize engagement. The longer a user is on a platform and the more they do on the platform, the more data the user generates. Tech companies and their marketing partners use this valuable data to target users with advertising.⁶¹ Gaming app companies employ teams of experts who specialize in user acquisition and retention.⁶² The

9

 ⁵⁵ Thorn. "Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking." (May 2021), <u>https://info.thorn.org/hubfs/Research/Responding%20to%20Online%20Threats 2021-Full-Report.pdf</u>.
 ⁵⁶ Thorn. "Understanding sexually explicit images, self-produced by children." (9 Dec. 2020), <u>https://www.thorn.org/blog/thorn-research-understanding-sexually-explicit-images-self-produced-by-children/.</u>
 ⁵⁷ Tmily A. Vogels et. al, *Teens and Cyberbullying 2022*, Pew Research Center, (Dec. 2022), <u>https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/.</u>
 ⁵⁸Bauman, S., & Baldasare, A., *Cyber aggression among college students: Demographic differences, predictors of distress, and the role of the university, 56 Journal of College Student Development 317 (2015), <u>https://doi.org/10.1353/csd.2015.0039</u>.*

⁵⁹van Geel M, Vedder P, Tanilon J. *Relationship Between Peer Victimization, Cyberbullying, and Suicide in Children and Adolescents: A Meta-analysis,* JAMA Pediatr. 2014;168(5):435–442. doi:10.1001/jamapediatrics.2013.4143 <u>https://jamanetwork.com/journals/jamapediatrics/fullarticle/1840250</u>.

⁶⁰Case 5:22-cv-00518-BO, *Epic Games: Complaint for Permanent Injunction*, (Dec. 19, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2223087EpicGamesComplaint.pdf.

 ⁶¹ See generally 5Rights Foundation. "Pathways: How digital design puts children at risk." (July 2021), <u>https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf</u>.
 ⁶² See, e.g., Leading User Acquisition in the quickly growing mobile games industry: Get to know Winnie Wen of Jam

City, Jam City (Nov. 15, 2021), https://www.jamcity.com/leading-user-acquisition-in-the-quickly-growing-mobile-

Testimony of Josh Golin, Fairplay, February 14, 2023

major social media platforms – including Facebook, Instagram, YouTube, and TikTok – have both in-house and external research initiatives focused on documenting and improving engagement, as well as utilizing neuromarketing and virtual reality techniques to measure effectiveness.⁶³

Engagement-maximizing design features prey upon minors' developmental vulnerabilities and can lead to significant harm. These features create risk for children because they can lead to problematic internet use and the associated harm. In addition, many of the techniques used to extend engagement create new risks and harms in their own right. They include: social manipulation design features; variable reward design features; and algorithmic content recommendation systems.

Social manipulation design features

Social manipulation design features leverage a minor's desire for social relationships to encourage users to spend more time and/or perform more activities on a website or service. These features are the hallmarks of social media platforms: follower, view, and like counts; interaction streaks; displays of the names of users who have commented, viewed, or liked a piece of content; and prompts that encourage a user to share with a larger audience by adding suggested new friends or making their account or posts public.

Younger adolescents have specific developmental needs for social connectedness and are particularly attuned to social validation.⁶⁴ Children develop a need to fit in with their peers around age 6⁶⁵ and the need to be noticed and admired by others around age ten.⁶⁶ Social

games-industry-get-to-know-winnie-wen-of-jam-city/; Mediation that supports everything your app business needs to scale, ironSource, https://www.is.com/mediation/; Mihovil Grguric, 15 Key Mobile Game Metrics That Developers MUST Track, udonis (Sept. 20, 2022), https://www.blog.udonis.co/mobile-marketing/mobile-games/key-mobile-game-metrics.

⁶³ See, e.g., Meta Careers, Shape the Future of Marketing with the Marketing Science Team, Meta (Sept. 19, 2018), <u>https://www.metacareers.com/life/come-build-with-the-facebook-marketing-science-team/</u>; Bob Arnold & Anton Miller, How Google's Media Lab Boosts YouTube Ad Results, AdAge (May 14, 2021),

https://adage.com/article/google/how-googles-media-lab-boosts-youtube-ad-results/2335796; TikTok Insights, TikTok for Business (2022), https://www.tiktok.com/business/en-US/insights; TikTok Ads Break Through Better than TV and Drive Greater Audience Engagement, TikTok for Business,

https://www.tiktok.com/business/library/TikTokDrivesGreaterAudienceEngagement.pdf; How Virtual Reality Facilitates Social Connection, Meta, https://www.facebook.com/business/news/insights/how-virtual-realityfacilitates-social-connection.

⁶⁴ Nicholas D. Santer et al., *Early Adolescents' Perspectives on Digital Privacy,* Algorithmic Rights and Protections for Children (2021) at 6, 30.

⁶⁵ In particular, between the ages of six and nine, children start to feel the need to fit in to peer social groups. See Jun Zhao et al., 'I Make Up a Silly Name': Understanding Children's Perception of Privacy Risks Online, CHI Conference on Human Factors in Computing Systems Proceedings (May 2, 2019), <u>https://doi.org/10.1145/3290605.3300336</u>.

⁶⁶ Zara Abrams, Why Young Brains Are Especially Vulnerable to Social Media, APA (Feb. 3, 2022), <u>https://www.apa.org/news/apa/2022/social-media-children-teens</u> ("Starting around age 10, children's brains undergo a fundamental shift that spurs them to seek social rewards, including attention and approval from their peers.").

Testimony of Josh Golin, Fairplay, February 14, 2023

acceptance evokes activation in the brain's reward center.⁶⁷ Further, minors' prefrontal cortex, which helps regulate responses to social rewards, is not as mature as adults'.⁶⁸ These factors all converge to create a feedback loop in which, because minors crave this social reinforcement, they seek it out, and ultimately are unequipped with the tools to protect themselves against the allure of "rewards" that these manipulative design features purportedly promise.

Social manipulation design features also exploit young people's tendency for social comparison and recreate, on a 24/7 basis, the high school cafeteria experience where everyone can instantly see who is popular and who is not. Features such as like and follower counts and comment displays induce anxiety in minors that they or their content may not be as popular as that of their peers. In the words of one high school student, "[1]f you get a lot of likes, then 'Yay,' you look relevant, but then if you don't get a lot of likes and/or views, it can completely crush one's confidence. Especially knowing that you're not the only one who's able to see it."⁶⁹ Snapchat streaks literally quantify the strength of users' relationships and create pressure on users to communicate with their friends on the app daily.⁷⁰ Teens report feeling obligated to maintain Snapstreaks to "feel more popular" and show that they "care about that person."⁷¹

Ultimately, these design features create strong incentives for young people to engage in potentially harmful behaviors. Their drive for social rewards "lead[s] to greater relinquishing of security in certain arenas to gain social validation and belonging, for example, disclosing publicly to participate in online communities and accrue large amounts of likes, comments, and followers."⁷² Young users quickly learn that they can improve their social media metrics by posting frequently and posting particularly provocative or risqué content.⁷³ Such posts can increase the risk of cyberbullying and sexual exploitation. In addition, the pressure to

⁶⁷ Eveline Crone & Elly A. Konijn, *Media Use and Brain Development During Adolescence*, 9 Nature Comm. 1, 4 (2018), <u>https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5821838/</u>.

⁶⁸ For example, adults "tend to have a fixed sense of self that relies less on feedback from peers" and "adults have a more mature prefrontal cortex, an area that can help regulate emotional responses to social rewards." Zara Abrams, Why Young Brains Are Especially Vulnerable to Social Media, APA (Feb. 3, 2022), https://www.apa.org/news/apa/2022/social-media-children-teens.

⁶⁹ Katie Joseff, Social Media Is Doing More Harm than Good, Common Sense Media (Dec. 17, 2021), https://www.commonsensemedia.org/kids-action/articles/social-media-is-doing-more-harm-than-good.
⁷⁰ Taylor Lorenz, *Teens Explain the World of Snapchat's Addictive Streaks, Where Friendships Live or Die*, Insider (Apr. 14, 2017, 1:58 PM), https://www.insider.com/teens-explain-snapchat-streaks-why-theyre-so-addictive-andimportant-to-friendships-2017-4; Lori Janjigian, *What I Learned After Taking Over My 13-Year-Old Sister's Snapchat for Two Weeks*, Business Insider (Aug. 4, 2016, 11:53 AM), <u>https://www.businessinsider.com/how-teens-are-usingsnapchat-in-2016.</u>

 ⁷¹ Id.
 ⁷² Nicholas D. Santer et al., Early Adolescents' Perspectives on Digital Privacy, Algorithmic Rights and Protections for Children (2021) at 6 (citing J.C. Yau & S. M. Reich, "It's Just a Lot of Work": Adolescents' Self-Presentation Norms

and Practices on Facebook and Instagram, 29 J. Res. on Adolescence 196, 196-209 (2019)). ⁷³ For example, Adolescent girls report feeling pressure to post sexualized selfies as a means of generating attention and social acceptance from their peers. Macheroni, G., Vincent, J., Jimenez, E. 'Girls Are Addicted to Likes so They Post Semi-Naked Selfies': Peer Mediation, Normativity and the Construction of Identity Online, 9 Cyberpsychology: Journal of Psychosocial Research on Cyberspace (May 1, 2015), <u>https://doi.org/10.5817/CP2015-</u> 1-5.

demonstrate popularity through high friend, follower, and like counts can lead children to accept friend requests from strangers, putting them at risk of predation.

Variable reward design features

One objective of persuasive design is to reduce friction so that platforms are easier to use, and so young people will keep using them. Low-friction variable rewards are highly effective at maximizing the amount of time users spend on the service. The psychology that renders these features effective is based on research that predates the internet by many years, beginning with experiments by renowned psychologist B.F. Skinner in the early 20th century.⁷⁴ Research by Skinner and others revealed that when test subjects – both humans and other animals – are rewarded unpredictably for a given action, they will engage in the action for a longer period of time than if the reward is predictable.⁷⁵ Specifically, the brain generates more dopamine in response to an uncertain reward than in response to an expected and reliable one.⁷⁶ The tendency of variable rewards to drive compulsive behavior is sometimes referred to as the "Vegas Effect," and is the primary mechanism at work in slot machines.⁷⁷ In the words of Nir Eyal, a consumer psychology expert who wrote the popular industry how-to *Hooked: How to Build Habit-Forming Products*, "[v]ariable schedules of reward are one of the most powerful tools that companies use to hook users."⁷⁸

One common example of variable rewards design features is the infinite or endless scroll mechanism with variable content. When a platform uses endless scroll, a user is continuously fed new pieces of content as they scroll down a feed or page, and they never know what might appear next. Harvard researchers Emily Weinstein and Carrie James explain in their recent book on teens and technology: "Apps like TikTok have an endless database of content to offer users. Some videos are pointless or boring or upsetting; others give a fleeting reward in the form of funny, relatable, or compelling content."⁷⁹ The pursuit of the next "rewarding" piece of content keeps users scrolling. As one 16-year-old told Weinstein and James, Snapchat is "so addictive because it's so easy to go on to the next thing.... And you never know what amazing thing could be on the next Story, and all you have to do is tap once and you get to the next thing...⁸⁰

 ⁷⁴ J. E. Staddon & D. T. Cerutti, *Operant Conditioning*, 54 Annual Review of Psychology 115 (2003), https://doi.org/10.1146/annurev.psych.54.101601.145124; B. F. Skinner, *Two Types of Conditioned Reflex: A Reply to Konorski and Miller*, 16 J. Gen. Psychology, 272 (1937), https://doi.org/10.1080/00221309.1937.9917951.
 ⁷⁵ Laura MacPherson, *A Deep Dive into Variable Designs and How to Use Them*, DesignLi (Nov. 8, 2018), https://designli.co/blog/a-deep-dive-on-variable-rewards-and-how-to-use-them/: Mike Brooks. *The "Veaas Effect"*

of Our Screens, Psychol. Today (Jan. 4, 2019), https://www.psychologytoday.com/us/blog/tech-happylife/201901/the-vegas-effect-our-screens.

⁷⁶ Anna Hartford & Dan J. Stein, Attentional Harms and Digital Inequalities, 9 JMIR Mental Health 2, 3 (Feb. 11, 2022), <u>https://pubmed.ncbi.nlm.nih.gov/35147504/</u>.

⁷⁷ Mike Brooks, The "Vegas Effect" of Our Screens, Psychol. Today (Jan. 4, 2019),

https://www.psychologytoday.com/us/blog/tech-happy-life/201901/the-vegas-effect-our-screens. ⁷⁸ Nir Eyal, *The Hook Model: How to Manufacture Desire in 4 Steps*, Nir and Far, https://www.nirandfar.com/howto-manufacture-desire/.

⁷⁹ Emily Weinstein & Carrie James, Behind Their Screens: What Teens Are Facing (And Adults Are Missing), MIT Press, at 33 (2022); see also GCFGlobal.org, Digital Media Literacy: Why We Can't Stop Scrolling, https://edu.gcfglobal.org/en/digital-media-literacy/why-we-cant-stop-scrolling/1/.
⁸⁰ /d. at 34.

Testimony of Josh Golin, Fairplay, February 14, 2023

All popular social media platforms, including those used heavily by minors such as TikTok, Snapchat, Instagram, and Facebook, feature endless scroll feeds strategically designed to intermittently surface content that users are algorithmically predicted to engage with. An internal TikTok document said that the app maximizes for two metrics: user retention and time spent.⁸¹ Similarly, a product manager for YouTube's recommendation system explained that the platform's recommendation algorithm "is designed to do two things: match users with videos they're most likely to watch and enjoy, and . . . recommend videos that make them happy. . . . [S]o our viewers keep coming back to YouTube, because they know that they'll find videos that they like there."82 And Adam Mosseri of Instagram said, "[W]e make a set of predictions. These are educated guesses at how likely you are to interact with a post in different ways.... The more likely you are to take an action, and the more heavily we weigh that action, the higher up you'll see the post."83

Tech companies know that variable rewards are a valuable tool to increase users' activity and time spent online and ultimately, to maximize profits. But they are similarly aware of the risks associated with these types of rewards. For example, in 2020, responding to internal research indicating that teen users had difficulty controlling their use of Facebook and Instagram, a Meta employee wrote to a colleague: "I worry that the driving [users to engage in more frequent] sessions incentivizes us to make our product more addictive, without providing much more value... Intermittent rewards are the most effective (think slot machines), reinforcing behaviors that become especially hard to extinguish."84 Ultimately, these sophisticated variable reward techniques prey upon minors' developmental sensitivity to rewards.

Algorithmic content recommendation systems

Algorithms designed to maximize engagement fill young people's feeds with the content that is most likely to keep them online, even when that means exposing them to a post, image, or video that is dangerous or abusive. Platforms such as YouTube, TikTok, and Instagram serve users content based on automated suggestions. Algorithms choose which content to suggest to children and teens based on the vast amount of data they collect on users, such as likes, shares, comments, interests, geolocation, and information about the videos a user watches and for how long. As described above, these algorithms are designed to extend engagement by discerning which pieces of content a user is most likely to engage with - not whether the content or overall online experience is beneficial to the user.85

13

⁸¹ Ben Smith, How TikTok Reads Your Mind, New York Times, (Dec. 5, 2021),

https://www.nytimes.com/2021/12/05/business/media/tiktok-algorithm.html. ⁸² Creator Insider, Behind the Algorithms - How Search and Discovery Works on YouTube, YouTube (Apr. 16, 2021), https://youtu.be/9Fn79qJa2Fc.

⁸³ Adam Mosseri, Shedding More Light on How Instagram Works, Instagram (June 8, 2021), https://about.instagram.com/blog/announcements/shedding-more-light-on-how-instagram-works. ⁸⁴ Spence v. Meta Platforms, N.D. Cal. Case No. 3:22-cv-03294 at 82 (June 6, 2022) (citing Facebook Papers: "Teen Girls Body Image and Social Comparison on Instagram - An Exploratory Study in the US" (March 2020), at p. 8). ⁸⁵ A former YouTube engineer observed: "recommendations are designed to optimize watch time, there is no reason that it shows content that is actually good for kids. It might sometimes, but if it does, it is coincidence." Orphanides, K.G. "Children's YouTube is still churning out blood, suicide and cannibalism." Wired, (March 23, 2018), https://www.wired.co.uk/article/youtube-for-kids-videos-problems-algorithm-recommend

Testimony of Josh Golin, Fairplay, February 14, 2023

Algorithmic recommendations can be particularly dangerous when they target children and teens' greatest vulnerabilities. Investigations have repeatedly demonstrated the way social media feeds deliver harmful mental health and eating disorder content to accounts registered to minors. A December 2022 report by the Center for Countering Digital Hate (CCDH) found that newly created TikTok accounts registered to teenagers that watched or liked videos about body image, mental health, or eating disorders received videos in their For You feed related to self-harm, suicide, or eating disorders within minutes.⁸⁶ These videos appeared on the accounts' For You feeds every 206 seconds on average. CCDH also studied the For You feeds of newly created TikTok accounts registered to teenagers that included the phrase "loseweight" in their usernames. Those accounts received videos about self-harm, suicide, or eating disorders in their For You feeds every 66 seconds on average.⁸⁷

Other reports have made similar findings: A 2021 *Wall Street Journal* investigation documented how TikTok users were served videos that encouraged eating disorders and discussed suicide.⁸⁸ The same year, Senator Richard Blumenthal's office created an account for a fake 13-year-old girl that "liked" content about dieting, and the account was served pro-eating disorder and self-harm content within 24 hours.⁸⁹ Young users' engagement with this harmful content is valuable to tech companies: Our 2022 report detailed how Meta profits from 90,000 unique pro-eating disorder accounts that reach 20 million people, one-third of whom are minors, some as young as nine.⁹⁰

Content recommendation algorithms also expose minors to videos of dangerous viral "challenges," which has tragically led to the serious injury and death of many young people. For example, media reports have documented how "the blackout challenge" on TikTok, in which young people hold their breath or choke themselves until they pass out, is responsible for the deaths of several children.⁹¹ Many families say that their children learned about the challenge through recommended videos on their For You feeds.⁹²

V. Apps, websites, and platforms target children with unfair surveillance advertising and influencer marketing techniques.

⁹¹Olivia Carville, *TikTok's Viral Challenges Keep Luring Young Kids to Their Deaths*, Bloomberg, (Nov. 30, 2022), https://www.bloomberg.com/news/features/2022-11-30/is-tiktok-responsible-if-kids-die-doing-dangerous-viralchallenges; Anne Marie Lee, *Child deaths blamed on TikTok 'blackout challenge' spark outcry, CBS News*, (Aug. 19, 2021), https://www.cbsnews.com/news/tik-tok-blackout-challenge-child-deaths/.

⁹²Michael Levenson and April Rubin, *Parents Sue TikTok, Saying Children Died After Viewing 'Blackout Challenge'*, New York Times, (July 6, 2022), <u>https://www.nytimes.com/2022/07/06/technology/tiktok-blackout-challenge-</u> <u>deaths.html</u>.

⁸⁶ Center for Countering Digital Hate, Deadly by Design: Tik Tok Pushes Harmful Content Promoting Eating Disorders and Self-harm into users' feeds, (Dec. 15, 2022), <u>https://counterhate.com/research/deadly-by-design/</u> ⁸⁷ Id.

 ⁸⁸ Wall Street Journal Staff, Inside TikTok's Algorithm: A WSJ Video Investigation, Wall Street Journal, (July 21, 2021), <u>https://www.wsi.com/articles/tiktok-algorithm-video-investigation-11626877477</u>.
 ⁸⁹Nihal Krishan, Senate office impersonates 13-year-old girl on Instagram to flag eating disorder content, Yahoo

News, (Sep. 30 2021), <u>https://www.yahoo.com/entertainment/senate-office-impersonates-13-old-</u> 212700515.html.

⁹⁰ Fairplay, *Designing for Disorder: Instagram's Pro-eating Disorder Bubble* at 1 (Apr. 2022), https://fairplayforkids.org/wp-content/uploads/2022/04/designing for disorder.pdf.

Digital platforms also harm children and teens through unfair digital advertising practices, including surveillance advertising and influencer marketing. These techniques make it harder for young people to recognize content as advertising designed to influence their behaviors and defend themselves against it, rendering them vulnerable to the influence of corporate actors that can collect and utilize data to target them with precision.

Children face pervasive and inappropriate advertising from a young age: According to one study, more than 95% of early childhood videos on YouTube contain ads, and one in five videos viewed by children 8 and under contained ads that were not age-appropriate, such as ads that featured violent or sexualized content.⁹³ Researchers have also found a high rate of age-inappropriate advertisements on preschool apps⁹⁴ and have found that the educational potential of children's apps is severely degraded by the high number of disruptive ads that appear, particularly on free apps that are more likely to be used by low-income children.⁹⁵

Surveillance advertising

Surveillance advertising – targeted advertising using personal data collected by websites and platforms – is the dominant form of marketing online. Programmatic data-driven advertising accounted for 90% of display ads in the U.S. last year.⁹⁶ This pervasive form of advertising draws on massive amounts of data about young people. By some estimates, advertisers already possess over 13 million data points about a child by the time they turn 13, despite the fact that the Children's Online Privacy Protection Act (COPPA) requires parental permission before sharing the personal information of children 12 and under with advertisers.⁹⁷ These data are drawn from countless daily activities, including web surfing, interacting with friends on social media, and recording messages and exchanging images and other communications on computers, phones, and tablets.⁹⁸ Smart home technologies allow companies to collect data on a young person's home life; extended reality (virtual, augmented, and mixed reality) devices can collect unique biometric data.

⁹³ Radesky, J. S., Schaller, A., Yeo, S. L., Weeks, H. M., & Robb, M.B. "Young kids and YouTube: How ads, toys, and games dominate viewing." *Common Sense Media*, (2020),

https://d2e111jq13me73.cloudfront.net/sites/default/files/uploads/research/2020_youngkidsyoutubereport_final-release_forweb.pdf. ⁹⁴ Meyer M, Adkins V, Yuan N, Weeks HM, Chang YJ, Radesky J. "Advertising in Young Children's Apps: A Content

³⁴ Meyer M, Adkins V, Yuan N, Weeks HM, Chang YJ, Radesky J. "Advertising in Young Children's Apps: A Content Analysis." J Dev Behav Pediatr, (Jan. 2019), <u>https://pubmed.ncbi.nlm.nih.gov/30371646/</u>.

⁹⁵ Meyer, M., Zosh, J.M., McLaren, C., Robb, M., McCaffery, H., Golinkoff, R.M., Hirsh-Pasek, K., & Radesky, J. "How educational are "educational" apps for young children? App store content analysis using the Four Pillars of Learning framework." *Journal of Children and Media*, (2021),

https://www.tandfonline.com/doi/abs/10.1080/17482798.2021.1882516?journalCode=rchm20. ⁹⁶ Meaghan Yuen, *Programmatic Digital Display Advertising in 2022: Ad Spend, Formats, and Forecast,* Insider Intelligence (May 23, 2022), <u>https://www.insiderintelligence.com/insights/programmatic-digital-display-ad-</u> <u>spending/</u>.

⁹⁷ SuperAwesome Launches Kid-Safe Filter to Prevent Online Ads from Stealing Children's Personal Data, SuperAwesome (Dec. 6, 2018), <u>https://www.superawesome.com/superawesome-launches-kid-safe-filter-to-</u>prevent-online-ads-from-stealing-childrens-personal-data/

prevent-online-ads-from-stealing-childrens-personal-data/. ⁹⁸ Wolfie Christl, Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions, Cracked Labs (June 2017),

https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf.

Testimony of Josh Golin, Fairplay, February 14, 2023

Kids and teens cannot appreciate the depth and breadth of these data collection systems, nor the way they are used to target them with precision. Younger children largely think about privacy in interpersonal terms, such as the ability to be left alone and control access to physical places.⁹⁹ As children get older, they may start to think about privacy in terms of freedom from surveillance at school or by the government, but they do not think about privacy in the sense that companies might use information about them to influence their purchasing choices, for example.¹⁰⁰

Ultimately, surveillance ads are inherently unfair when targeted to children. As Fairplay, Global Action Plan, and Reset Australia described in a report about Facebook:

On the one side is a child, poorly equipped to distinguish between advertising and information, especially within digital contexts. On the other, Facebook with its vast troves of data about the child, including but not limited to their browsing history, mood, insecurities, their peers' interests, and more. This power imbalance makes surveillance advertising inherently more manipulative than contextual digital advertising, let alone traditional analogue advertising.¹⁰¹

As with algorithmically recommended content, surveillance ads can be used to target and exacerbate young people's vulnerabilities. Leaked documents from Facebook revealed in 2017 that the company told advertisers it could help them target teens at moments when they are feeling specific emotions, such as "silly," "defeated," "overwhelmed," "useless" and "a failure."¹⁰² Facebook Australia told advertisers it could specify when teens are likely to experience certain moods, sharing that "earlier in the week, teens post more about 'anticipatory emotions' and 'building confidence,' while weekend teen posts contain more 'reflective emotions' and 'achievement broadcasting."¹⁰³

This capability allows marketers to target vulnerable young people with ads for harmful products. Ads for risky "Flat Tummy Teas" and dangerous exercise routines target young women on Instagram. Early digital marketing campaigns for Juul vaping products were deliberately targeted at young audiences.¹⁰⁴ Researchers were able to target ads to teenagers

⁹⁹ Kaiwen Sun et al., They See You're a Girl if You Pick a Pink Robot with a Skirt: A Qualitative Study of How Children Conceptualize Data Processing and Digital Privacy Risks, CHI Conference on Human Factors in Computing Systems (May 2021), <u>https://dblp.org/rec/conf/chi/SunSASGR521</u>; Priya Kumar et al., No Telling Passcodes Out Because They're Private: Understanding Children's Mental Models of Privacy and Security Online, 1 Proceedings of the ACM on Human-Computer Interaction 64, (Nov. 2017), <u>https://pearl.umd.edu/wp-content/uploads/2017/08/kumar-</u> <u>etal-2018-CSCW-Online-First.pdf</u>.

¹⁰⁰ Mariya Stoilova et al., *Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy*, 8 Media and Commc'n 197, 200, (2020), <u>http://dx.doi.org/10.17645/mac.v8i4.3407</u>.

 ¹⁰¹ Yi-ching Ho, E., Farthing, R., *How Facebook still targets surveillance ads to teens*, Reset Australia, Fairplay, and Global Action Plan (Nov. 2021), <u>https://fairplayforkids.org/wp-content/uploads/2021/11/fbsurveillancereport.pdf</u>.
 ¹⁰² Sam Machkovech, *Report: Facebook Helped Advertisers Target Teens Who Feel "Worthless"*, ArsTechnica (May 1, 2017), <u>https://arstechnica.com/information-technology/2017/05/facebook-helpedadvertisers-target-teens-who-feel-worthless</u>.

¹⁰³ Id.

¹⁰⁴ Jidong Huang et al., *Vaping versus JUULing: how the extraordinary growth and marketing of JUUL transformed the US retail e-cigarette market,* 28 Tobacco Control 146, 150 (Feb. 22, 2019),

https://doi.org/10.1136%2Ftobaccocontrol-2018-054382 ("JUUL was one of the first major retail e-cigarette

Testimony of Josh Golin, Fairplay, February 14, 2023

on Facebook based on their interests in gambling, alcohol, and dieting.¹⁰⁵ While Meta announced in 2021 that they were restricting advertisers' ability to target teens based on their interests, this change was misleading, as the company's ad targeting algorithm still used the data it collected on young people to determine who is most likely to be vulnerable to a given ad.¹⁰⁶

Even in cases where the products aren't as harmful as alcohol or dieting aids, surveillance advertising exploits children. As Common Sense notes, "Kids may be profiled as gamers, impulsive purchasers, or anxious oversharers – and then unfairly targeted by ads that encourage more of these things."¹⁰⁷

Influencer marketing

Product placement and host-selling are not permitted on children's television, where regulations require clear separation between content that is advertising and content that is not. The online marketing ecosystem does not have similar rules, and as a result, advertising and entertainment and informational content are deeply intertwined.

One of the ways that marketers reach kids and teens online is by advertising products through influencers and trusted fictional characters. This method of advertising is highly appealing to marketers because it is seen as more "authentic" and it capitalizes on the relationships that kids and teens form with the characters and media figures they see online. This advertising sector is huge and getting bigger. Market research shows that influencer marketing is currently growing by billions of dollars annually.¹⁰⁸ Influencer marketing reaches even the youngest kids online: "kidfluencers" on YouTube receive millions of views on videos of themselves unboxing and showing off new toys from brands and marketers.

Research demonstrates that influencer marketing overcomes children and teenagers' nascent cognitive ability to understand and defend themselves against advertising. For example, young people identify closely with these media characters and figures and develop feelings or

brands that relied heavily on social media to market and promote its products."); Julia Cen Chen-Sankey et al., Ecigarette Marketing Exposure and Subsequent Experimentation Among Youth and Young Adults, 144 Pediatrics at 8 (Nov. 2019), <u>https://doi.org/10.1542/peds.2019-1119</u>; *see also* Erik Larson et al., *Juul Reaches \$439 Million Settlement Over Marketing to Kids*, Bloomberg Law, (Sept. 6, 2022), <u>https://news.bloomberglaw.com/health-law-</u> and-business/juul-reaches-439-million-multi-state-settlement-over-marketing.

and-business/juul-reaches-439-million-multi-state-settlement-over-marketing. ¹⁰⁵ Farthing, Rys, et al., *Profiling Children for Advertising: Facebook's Monetisation of Young People's Personal Data*, Reset Australia, (April 2021), <u>https://au.reset.tech/uploads/resettechaustralia_profiling-children-for-advertising-</u> 1.ndf.

<u>1.pdf</u>. ¹⁰⁶ *Id*. In February 2023, Meta announced yet another change to its ad targeting for teens and now claims it will not use teens interests or online activities at all for the targeting of ads to minors. As of this writing, Fairplay has not had the opportunity to verify this claim.

 ¹⁰⁷ Joseph Jerome and Ariel Fox Johnson, *AdTech and Kids: Behavioral Ads Need a Time-Out, Common Sense*,
 (2021), <u>https://d2e111jg13me73.cloudfront.net/sites/default/files/uploads/AdTech%20and%20Kids.pdf</u>.
 ¹⁰⁸ Traackr, 2022 Influencer Marketing Impact Report at 2, (2022),

https://www.traackr.com/content/influencermarketing-impact-report-2022; State of Influencer Marketing 2022, Influencer Marketing Hub at 10, (2022),

https://influencermarketinghub.com/ebooks/Influencer Marketing Benchmark Report 2022.pdf.

friendships known as parasocial relationships.¹⁰⁹ As a result of these relationships, kids and teens have difficulty responding to content from a beloved character or creator as an advertisement,¹¹⁰ and can therefore be unduly influenced by marketers. As Fairplay outlined in its comments to the Federal Trade Commission last year, the existing system of disclosures – even when it is followed – does very little to alert kids and teens to the massive amounts of advertising content they encounter online every day.¹¹¹

This form of stealth marketing negatively impacts kids and teens. Children who watch unboxing videos are more likely to nag their parents for products and throw a tantrum if the answer is "no" than when they watch regular commercials.¹¹² In internal Meta research leaked by Frances Haugen, teens specified that influencers and their materialistic, over-the-top "money for nothing" – or effortlessly rich – lifestyles triggered social comparisons and contributed to young people feeling bad about themselves. The research emphasized the cumulative effect of influencers in each app session, multiplying their effect. In addition, their friends mimic celebrities' beauty and fashion standards, further compounding the effects of one piece of content."¹¹³

VI. Congress must take action to protect young people online.

When kids are in digital spaces for learning, socializing, and relaxing, they deserve the opportunity for the most positive experience, designed in a way that understands and supports their unique ways of seeing the world. They should be able to explore in developmentally-appropriate ways without being manipulated into spending more time or targeted by algorithms that amplify harmful content.

We cannot continue to hope that tech platforms will unilaterally disarm in the race for young people's valuable attention. Nor can we expect young people to extract themselves from the

¹⁰⁹ Amanda N. Tolbert & Kristin L. Drogos, *Tweens' Wishful Identification and Parasocial Relationships With YouTubers*, 10 Frontiers In Psychology 1, (2019),

<u>https://www.frontiersin.org/articles/10.3389/fpsyg.2019.02781/full</u>; Frans Folkvord, K.E. Bevelander & Esther Rozendaal, et al., *Children's bonding with popular YouTube vloggers and their attitudes toward brand and product endorsements in vlogs: an explorative study*, 20 Young Consumers Insight And Ideas For Responsible Marketers (2019), <u>https://doi.org/10.1108/YC-12-2018-0896</u>.

¹¹⁰ Emmelyn Croes & Jos Bartels, Young adults' motivations for following social influencers and their relationship to identification and buying behavior, 125 Computers In Human Behavior at 7, (2021),

https://doi.org/10.1016/j.chb.2021.106910; 4 Brigitte Naderer, Jörg Matthes & Stephanie Schäfer, Effects of disclosing ads on Instagram: the moderating impact of similarity to the influencer, 40 International Journal of Advertising 686, 687-88 (2021).

¹¹¹ See generally Comments of Fairplay, Alexander Neville Foundation, et al. in the Matter of Protecting Kids from Stealth Advertising in Digital Media (filed July 18, 2022), <u>https://fairplayforkids.org/wpcontent/uploads/2022/07/influencer-comments.pdf</u>.

¹¹² Harsha Gangadharbatla & Deepti Khedekar, The Role of Parental Mediation and Persuasion Knowledge in Children's Consumption of Unboxing Videos, 22 Advertising & Society Quarterly (2021), https://muse.jhu.edu/article/813891.

¹¹³ The Wall Street Journal, *Teen Girls Body Image and Social Comparison on Instagram – An Exploratory Study in the U.S.,* (Sep. 29, 2021) <u>https://s.wsj.net/public/resources/documents/teen-girls-body-image-and-social-comparison-on-instagram.pdf</u>.

exploitative platforms where their friends are, or expect overworked parents to navigate confusing settings across multiple platforms and monitor every moment their kids are online.

The last time Congress passed a law to protect children online was 25 years ago. The digital landscape has changed dramatically, in many unforeseen ways, since the passage of the Children's Online Privacy Protection Act in 1998 when smart phones, YouTube, social media, multiplayer gaming with voice chat, and virtual reality didn't even exist. In addition, COPPA only covers children until they turn 13 and has failed to effectively keep kids ages 12 and under off of platforms like Snapchat, Instagram and TikTok, leaving significant demographics vulnerable to exploitation and harm. Congress's continued inaction has emboldened Big Tech to develop an exploitative business model without considering or mitigating its harmful effects on children and teens. Consequently, the social media platforms that define youth culture and norms and shape children's values, behavior, and self-image were developed with little to no thought given to how young people might be negatively affected.

We cannot expect a 25-year-old framework to adequately protect children from today's sophisticated persuasive technologies powered by big data and machine learning or in the rapidly developing metaverse. We need new legislation that puts brakes on this harmful business model and curbs dangerous and unfair design practices.

At a minimum, such legislation should:

- Extend privacy protections to teens. Currently, COPPA only covers children until their 13th birthday. It is critical to limit the collection of adolescents' data, which fuels harmful recommendations and puts young people at risk of privacy harms.
- Ban targeted advertising to children and teens to protect them from harmful marketing targeted to their vulnerabilities. Surveillance ads not only take advantage of young people's developing capacities and sell them on harmful products, but they also incentivize tech platforms to prioritize engagement over safety.
- 3. Require tech companies to make the best interests of children and teens a primary consideration in the design and operation of their platforms, including their algorithms. It is important that such liability be broad enough to capture current harmful practices, such as quantified popularity, as well as emerging features and products. The latter is particularly important given the rapid development of metaverse applications targeted to young people.¹¹⁴ Companies should have a duty to prevent and mitigate harms to young people before new features or products are released.
- 4. Prohibit the use of dark patterns, which are used to undermine young people's autonomy and manipulate them into spending more time or money on a platform.
- 5. Impose transparency requirements, including access to algorithms, that enable outside researchers to better understand the impacts of social media on young people. We

¹¹⁴ See, e.g, Salvador Rodriguez, *Meta Pursues Teen Users as Horizon Metaverse App Struggles to Grow*, The Wall Street Journal (Feb. 8, 2023) <u>https://www.wsj.com/articles/meta-to-revamp-horizon-metaverse-app-plans-to-open-for-teen-use-as-soon-as-march-11675749223</u>.

shouldn't have to rely on courageous whistleblowers like Frances Haugen to understand how social media platforms are impacting our youth.

- Require minors' privacy and account settings to be on the most protective by default, rather than putting the onus on youth or their parents to navigate a maze of confusing settings just to have a safer, more age-appropriate experience.
- Have a clear and effective enforcement mechanism, such as a division at the FTC, solely dedicated to protecting young people and their privacy online.

The good news is that two bills which together would do all of the above, the Kids Online Safety Act and the Children and Teens' Online Privacy Protection Act, advanced out of the Commerce Committee with broad bipartisan support last July – the first such legislation to advance out of committee in more than two decades. The Committee votes came on the heels of a number of important hearings with whistleblowers, child development experts, and tech executives in the Senate Judiciary and Commerce Committees and House Energy and Commerce Committee, which established a clear record of harm and the need for new online protections for young people.

The bad news, of course, is that neither bill became law or even received a floor vote. And every day that the status quo continues, children are suffering – and even dying – from preventable harms.

We've named the problem and debated the solutions. Now it's time to build on last year's momentum and disrupt the cycle of harm by passing privacy and safety-by-design legislation. Let's make 2023 the year that Congress finally takes a huge step toward creating the internet children and families deserve.

Thank you again for having me here today and I look forward to discussing all of this with you.

93

LOG OFF

Written Testimony of Emma Lembke, Founder and Executive Director of the LOG OFF Movement

United States Senate Committee on the Judiciary: Protecting Our Children Online

February 14, 2023

My name is Emma Lembke. I am originally from Birmingham, Alabama. I am currently a college sophomore studying Political Science at Washington University in St. Louis. I am honored and humbled to be here today.

I created my first social media account on Instagram when I was 12. I was in 6th grade and I was the last in my friend group allowed on social media platforms. At the time, I distinctly remember watching these apps pull my friends' attention away from games of tag and down, towards their screens. To 12-year-old me, these platforms almost seemed magical; tools that could deepen society's connective, expressive, and exploratory capabilities.

It felt as though I, a girl from Birmingham, Alabama, had the world at my fingertips, but as I began to spend more time on these platforms, I was met with a harsh reality. Social media was not magic. It was an illusion, a carefully designed product predicated on maximizing my attention at the cost of my well-being.

As my screen time steadily increased, my mental and physical health suffered. The constant quantification of my worth through likes, comments, and followers increased my anxiety and deepened my depression. As a young woman, being exposed to unrealistic body standards and harmful recommended content severely damaged my sense of self and led me towards disordered eating. I became the living embodiment of <u>Facebook's own 2019</u> <u>internal research finding</u> that their platforms made body image issues worse for one in three teen girls.

No matter the harm I incurred, addictive features like the endless scroll and autoplay pulled me back into the online world where I continued to suffer. And there, I remained for over three years, scrolling mindlessly for 5-6 hours a day. I eventually reached a personal breaking point in the 9th grade that caused me to temporarily remove social media apps

from my device. I am still recovering today from the damage caused by social media and hyper aware that many of its effects are long lasting, if not permanent.

Senators, my story does not exist in isolation– it is a story representative of my generation, Generation Z. As the first digital natives, we grew up alongside technology. We have never known a world without the internet. Every answer has been a Google search away, every moment captured on Facebook or Instagram.

To be clear, social media can enhance our connective, expressive, and exploratory capabilities, but we are only just beginning to understand the consequences associated with growing up online. Yet, it is from our lived experience as Generation Z - the generation most harmed - that we can begin to build the most promising solutions. Decision makers from other generations must hear from us to fully understand the challenges and opportunities associated with being a young person in the digital world. It is only when young people are given a space at the table that effective solutions can emerge and safer online spaces can be created. The power of youth voices in the space is far too great to continue to be ignored.

This is why, as a senior in high school, after years of researching and reflecting on my own relationship with social media, I founded the LOG OFF Movement. I knew a community had to be created by young people for young people to tackle the complexities of social media and its impact on younger generations.

Through LOG OFF, I have engaged with youth around the world who have shared their experiences of harm with me. I've listened to stories of unwanted direct messages, vicious cyberbullying, and dangerous pro-anorexia rabbit holes. While our stories may differ, as young people we share the frustration of being portrayed as passive victims of Big Tech when in reality, we are ready to be included as active agents of change; rebuilding new, and safer online space for the next generation. Ten years from now social media will not be what it is today, it will be what people of my generation build it to be. We want to build it differently, we want to build it right.

I came here today as the representative for those young changemakers. To be the voice not just of those of my generation who have been harmed or who are currently struggling, but as a voice for all the 12-year-old girls yet to come. The genie is out of the bottle, and screen time across younger generations is only increasing, with <u>the number of US teenagers</u>

online continuously almost doubling from 2015 to 2018: 24% to 45%. In 2020, 81% of 14 to 22-year-olds said they used social media either "daily" or "almost constantly."

As a society, we will never go back to a time where social media does not exist, nor should we. But make no mistake, unregulated social media is a weapon of mass destruction that continues to jeopardize the privacy, safety, and wellbeing of all American youth. This harm does not stop at the borders of the United States, this is a global crisis. The United States has a unique opportunity to lead the world in putting a stop to predatory and targeted actions by Big Tech against the world's most vulnerable.

It's time to act and, Senators, I urge you to meaningfully regulate these companies not just *for* my generation but *with* my generation. Integrating our lived experience into the regulatory process is essential to getting it right.

Thank you for having me here today. I look forward to answering your questions.

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

for the

UNITED STATES SENATE COMMITTEE ON THE JUDICIARY Protecting Our Children Online

February 14, 2023

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

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

Those who would protect our youth are overburdened and under-resourced, which makes children vulnerable. Our nation's young people are unable to escape from the bombardment of posts, reels, and online social interaction. A major disadvantage of our global society is that any offender can reach any victim, anywhere in the world, through any app or gaming platform. We live in a world where everyday tasks increasingly are accomplished through apps, from shopping, to making a flight reservation, to – sadly – even children buying drugs.

I am here today as the CEO of Raven, an advocacy group comprised of 14 professionals, including nine retired Internet Crimes Against Children (ICAC) Task Force Commanders, who have committed their lives to the advocacy and protection of children. The Internet Crimes Against Children Task Force Program (ICAC program) helps state and local law enforcement agencies develop an effective response to technology-facilitated child sexual exploitation and Internet crimes against children. The ICAC program is a national network of 61 coordinated task forces, with at least one in each state, representing more than 4,700 federal, state, and local law enforcement and prosecutorial agencies. These agencies are engaged in both proactive and reactive investigations, forensic investigations, and criminal prosecutions. This ICAC program also encompasses training and technical assistance, victim services, and community education.¹

96

¹ The ICAC Task Force program was developed in 1998 response to the increasing number of children and teenagers using the Internet, the proliferation of child sexual abuse images available electronically, and heightened online activity by predators seeking unsupervised contact with potential underage victims. The Providing Resources,

I am retired from the New Jersey State Police, where I served as the Commander of the Internet Crimes Against Children task force from 2015 to 2021. I personally experienced the struggles of how best to protect our children online. We witnessed children targeted by offenders across all platforms – no social media or gaming platform was safe, from apps such as Snapchat, Twitter, Kik, Telegram, Discord, LiveMe, and Meetme, to gaming platforms and online games such as Minecraft, Roblox, and Fortnite. And these represent just a fraction of the places where offenders regularly interact with children. If the platform allows individuals to chat, or a way to share photographs and videos, I assure you there is a very real danger that offenders are using that access to groom or sexually exploit minors. Sadly, in addition to sexual exploitation, the platforms allow children to buy drugs such as Fentanyl.²

Our children's world has become focused on "likes," followers, and views, and in this way social media exploits vulnerabilities in our children's psychology. In an interview with Axios, the former President of Facebook stated, "That means that we needed to sort of give you a little dopamine hit every once in a while, because someone liked or commented on a photo or a post or whatever ... It's a social-validation feedback loop ... You're exploiting a vulnerability in human psychology ... [The inventors] understood this, consciously, and we did it anyway."³

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

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

While sending compliments, virtual currency, gift cards, and other incentives are certainly part of grooming, today's offenders do even more to access children's trust. Offenders research children to know what they like, and do not like, what music they listen and so on. The offender will then mirror their words and repeat the exact language. The child then will see someone who

Officers, and Technology to Eradicate Cyber Threats to Our Children Act ("the PROTECT Act") of 2008, (P.L. 110-401, codified at 42 USC 17601, et seq.), authorized the ICAC program through FY 2013. On November 2, 2017, the Providing Resources, Officers, and Technology to Eradicate Cyber Threats to (PROTECT) Our Children Act of 2017 was signed into law, reauthorizing the ICAC Task Force Program through FY 2022. More information is available at <u>https://www.icactaskforce.org/</u>.

² https://ktla.com/news/local-news/mother-mourns-sons-death-from-fentanyl-laced-drugs-purchased-on-snapchat/.
³ https://www.axios.com/2017/12/15/sean-parker-facebook-was-designed-to-exploit-human-vulnerability-1513306782

is just like them. Chat forums on Tor share success stories on successfully grooming children of all ages. Each offender will attempt to groom hundreds of children using various techniques beyond just sending a picture or a video. We discuss numerous "in real life" dangers in school curriculums, yet online grooming is not part of it.

As the New Jersey ICAC Commander, I struggled with the significant increases in investigations, arrests, and victims we faced each year. For example, in 2015 we received 2,315 Cybertips and made 125 arrests, and by the end of 2019 we had 8,000 Cybertips and we made 420 arrests. We understood the importance of trying to keep up, but even creative attempts to "do more with less" became unsustainable. And this was prior to COVID, when screentime increased substantially and cemented our children's reliance on apps. These challenges were frustratingly present with every ICAC task force across the United States. The most staggering increase we faced was self-generated CSAM cases – children taking sexual images of themselves as the request of offenders. These were not images of older teens sending photos of themselves to their boyfriends and girlfriends – we began to see images of 7, 8, and 9-year-olds in sexual poses. The online landscape is horrifying because offenders know this is where our children live, and they recognize there are not enough safeguards to keep them at bay.

During one case, I received a call from a Child Advocacy Center in another state. The advocate told me a mother had just arrived with her 8-year-old daughter after she found sexual abuse videos on the child's phone. An offender had obtained a sexually abusive video of an 11-year-old girl, and then used that video to coerce 60 children to share sexually explicit videos of themselves. This included a video of a 12-year-old girl abusing her 1½-year-old brother. These child victims were located throughout the United States and Canada and were using a popular live-streaming app. This is one example of thousands of cases throughout the United States and the globe.⁴

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

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

⁴ https://www.app.com/story/news/crime/2019/09/24/lakewood-sex-offender-had-more-than-1-000-images-child-porn-his-iphone-feds-say/2435710001/.

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

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

As noted above, the sheer volume of Cybertips also prevents law enforcement from pursuing proactive investigative effort that would efficiently target the most egregious offenders. For example, peer-to-peer file sharing investigations and operations used to allow ICAC Task Forces to efficiently locate and apprehend hands-on offenders.⁶ In the last 90 days, alone, there have been 99,172 IP addresses throughout the United States that have distributed known CSAM images and videos through peer-to-peer networks. Yet only 782 - less than 1% - are being investigated (see Exhibit 1). Consistently, 75% of these cases have resulted in successful prosecutions. Significantly, the most rigorous studies involving interviews with offenders have shown that between 57% and 85% of individuals arrested for these crimes have committed undetected sexual abuse of minors; on average, those offenders have assaulted between 10 to 13 victims.⁷ Due to the overwhelming volume of Cybertips, law enforcement is simply not investigating peer-to-peer to the degree that it wants and should.

EXHIBIT 1

⁵ Reactive investigations take place when law enforcement receives information, such as a CyberTip, that a crime has occurred. A proactive investigation involves the use of intelligence to try to identify potential offenders.

⁶ https://www.nj.gov/njsp/news/2016/20160818.shtml

⁷ https://www.ojp.gov/ncjrs/virtual-library/abstracts/butner-study-redux-report-incidence-hands-child-victimizationchild.



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 14year-olds. All of these undercover investigations are performed using social media apps or online ads that solicit the sexual assault of children. When arrests are made, investigators rarely find it is the first time the offender has traveled to sexually abuse a child.

These offenders bring drugs, alcohol, sex toys, and other paraphernalia. In one an offender brought a dog leash and collar so he could be "walked" by a 12-year-old.⁸ Task forces throughout the U.S. would conduct these operations on a routine basis, and they were very successful. The North Florida ICAC task force, for example, conducted 48 of these operations, arresting thousands of individuals, and obtained a conviction rate of 98.7%. Unfortunately, task forces are no longer able to perform these types of operations - they are resource intensive, and the volume of reactive cases prohibits it.

The Darknet, including Tor, has become the newest online haven for child exploitation.9 Some forums and boards contain the most abusive child exploitation videos and images law enforcement has encountered. Chat forums allow offenders to create "best practices" on how to groom and abuse children effectively. A post named the "Art of Seduction" that explained how to "seduce" children was read more than 54,000 times. Other posts discuss the best way to introduce sexual activity to children without alarming them or offer such topics as "Thoughts on having oral sex with 0-2-year-olds." These conversations are horrific, yet Tor is easily downloaded as a web browser, and children and teens can install it on their phones and begin accessing it within minutes.

100

 ⁸ <u>https://www.nj.gov/oag/newsreleases19/pr20190424a.html</u>.
 ⁹ The Dark Net is an encrypted portion of the internet that is not indexed by search engines where users can communicate anonymously without divulging identifying information, such as a user's location. Tor is one network on the Dark Net.

In one undercover operation a registered sex offender paid to sexually abuse an 11-year-old, spoke about how he was able to victimize his two-year-old nephew, and described how he groomed children into providing him with child sexual abuse videos.¹⁰ The offender sent screen shots of his texts with children with whom he had connected using Kik, which revealed his technique for convincing them to send him sexually explicit material. He admitted sexually assaulting a massage therapist and indicated he wanted to kidnap an eight-year-old child, but he was afraid of being caught.

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

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

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

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

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

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

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

102



Written Testimony of Mitch Prinstein, PhD, ABPP Chief Science Officer American Psychological Association *Protecting Our Children Online* Before the U.S. Senate Committee on Judiciary

February 14, 2023

Chairman Durbin, Ranking Member Graham, and members of the Judiciary Committee, thank you for the opportunity to testify today on the online dangers facing our children and teens. I am Dr. Mitch Prinstein, Chief Science Officer at the American Psychological Association (APA). APA Services, Inc. is the companion organization of the American Psychological Association, which is the nation's largest scientific and professional nonprofit organization representing the discipline and profession of psychology, as well as over 146,000 members and affiliates who are clinicians, researchers, educators, consultants, and students in psychological science. Through the application of psychological science and practice, our association's mission is to use psychological science and information to benefit society and improve lives.

I am grateful you have called attention to youth and the online environment. Our youth are struggling in many ways, largely due to our society's failure to adequately attend to child and adolescent mental health.

My testimony is broken down into the following sections to help inform the Committee about the complexities of the challenges before us and to help shape policy solutions:

٠	Overview	pg. 2
•	Online/ Social Media Behaviors and Youth Mental Health	pg. 6
•	Psychological Effects of Lost Opportunities While Youth Are Online	pg. 17

APA.ORG APASERVICES.ORG Advocating for APA members and psychology

 750 First Street, NE
 202.336.5800

 Washington, DC 20002-4242
 202.336.6123 TDD

1



Potential Solutions and Policy Implications

pg. 18

Overview

Today, we are seeing the repercussions of our underinvestment and lack of focus on children's mental health. Depression rates for teens doubled between 2009 and 2019 and suicide is the second leading cause of death for U.S. youth, up 4% since 2020, with one in five teens considering suicide during the pandemic and eating disorder emergency room admissions for girls 12 to 17 years old doubling since 2019¹. Furthermore, since the start of the pandemic, over 167,000 children have lost a parent or caregiver to the virus². This kind of profound loss can have significant impacts on the mental health of children, leading to anxiety, depression, trauma, and stress-related conditions³. Faced with such data, in December 2021, the U.S. Surgeon General issued an advisory calling for a unified national response to the mental health challenges young

¹Radhakrishnan, L. (2022). Pediatric Emergency Department Visits Associated with Mental Health Conditions Before and During the COVID-19 Pandemic — United States, January 2019–January 2022. MMWR. Morbidity and Mortality Weekly Report, 71(8). <u>https://doi.org/10.15585/mmwr.mm7108e2</u>; Curtin, S. (2022). Vital Statistics Rapid Release Provisional Numbers and Rates of Suicide by Month and Demographic Characteristics: United States, 2021. https://www.cdc.gov/nchs/data/vsrr/vsrr024.pdf; Daly, M. (2021). Prevalence of Depression Among Adolescents in the U.S. From 2009 to 2019: Analysis of Trends by Sex, Race/Ethnicity, and Income. Journal of Adolescent Health. <u>https://doi.org/10.1016/j.jadohealth.2021.08.026</u>; Suicide. (n.d.). National Institute of Mental Health (NIMH). Retrieved February 10, 2023, from

https://www.nimh.nih.gov/health/statistics/suicide#%3A~%3Atext%3DSuicide%20is%20a%20Leading%20Cause% 20of%20Death%20in%20the%20United%20States%2C-

According%20to%20the%26text%3DSuicide%20was%20the%20second%20leading%2Cages%20of%2035%20and %20244; Yard, E. (2021). Emergency Department Visits for Suspected Suicide Attempts Among Persons Aged 12– 25 Years Before and During the COVID-19 Pandemic — United States, January 2019–May 2021. MMWR. Morbidity and Mortality Weekly Report, 70(70(24);888–894). <u>https://doi.org/10.15585/mmwr.mm7024e1</u>. ² Hidden Pain: Children Who Lost a Parent or Caregiver to COVID-19 and What the Nation Can Do To Help Them | COVID Collaborative. (n.d.). Www.covidcollaborative.us. <u>https://www.covidcollaborative.us/initiatives/hiddenpain</u>.

³ Almeida, I. L. L., Rego, J. F., Teixeira, A. C. G., & Moreira, M. R. (2021). Social isolation and its impact on child and adolescent development: a systematic review. Revista paulista de pediatria : orgao oficial da Sociedade de Pediatria de Sao Paulo, 40, e2020385, https://doi.org/10.1590/1984-0462/2022/40/2020385.

APA.ORG
 State
 <



people are facing ⁴. The rarity of such advisories further underscores the need for action to help stem the mental health crisis of children and adolescents.

There are many reasons why youth are experiencing this crisis today, and it is likely that there are simultaneous contributors to the outcomes presented above. Today, we are here to talk about whether youths' engagement with social media, and other online platforms, may be a relevant factor. Many psychological scientists, including myself and my colleagues, have been asking this same question for years. We seek to understand how this new context in which youths' social interactions occur may be related to development, including potential benefits or risks that may be conferred by the online environment. As the discipline with expertise on all of human behavior, our work has been broad in scope; and to date, our focus has been on the adolescent period, during which more complex and mature behaviors are developed through intricate and precise interactions among neural, biological, social, contextual, and social systems. Today, although this remains a relatively nascent body of research, I would like to share what we know so far, so policymakers, educators, parents, caregivers, and youth can learn from what we are beginning to discover and make choices that will ensure the safety of youth.

In this testimony, I outline emerging research with findings that have begun to suggest possible benefits, and as well as possible adverse effects of technology and social media use on adolescent development. I also present legislative and regulatory solutions that if enacted, would represent positive steps towards learning more about, and hopefully solving this problem. I am calling for new legislation and regulations that increase research funding and provide education on how children can use online platforms without experiencing the most harmful impacts; legislation that creates a requirement that social media companies protect the well-being of child users; legislation that prohibits problematic business practices and prevents companies from tricking and manipulating users; and bills that provide more leverage for federal regulators to

3

APA.ORG APASERVICES.ORG 750 Advocating for APA members and psychology Wa

 750 First Street, NE
 202.336.5800

 Washington, DC 20002-4242
 202.336.6123 TDD

⁴ Richtel, M. (2021, December 7). Surgeon General Warns of Youth Mental Health Crisis. The New York Times. <u>https://www.nytimes.com/2021/12/07/science/pandemic-adolescents-depression-anxiety.html#:~:text=The%20United%20States%20surgeon%20general.</u>



clamp down on known harmful impacts while building internal expertise to prepare to tackle newly discovered harms. APA supported these efforts in past Congresses and commits to work to see these proposals enacted because, as I present below, scientific data are beginning to suggest areas of serious concern that must not be allowed to continue unchecked.

Before we discuss specific impacts of online platforms or solutions, it is important to acknowledge that causal data are not available for many of these issues, since the experimental designs needed to make cause-and-effect statements would be considered unethical or require access to currently inaccessible data. This underscores the need for increased access to data and funding for high-quality research. However, as with non-causal research revealing the effects of childhood adversity on mental health, or the effects of combat on PTSD among veterans, extant, rigorous science can nevertheless allow us to reach reasonable conclusions that can shape policy.

It also is important to acknowledge that technology and social media may not, in themselves, be problematic for child development, as each device and platform offers a multitude of features and communication opportunities that users can choose from. Extensive research has demonstrated that the amount of screentime alone is not likely associated with negative psychological outcomes among youth ⁵. Moreover, not all youth exposed to identical stimuli are affected in the same ways. Thus, the most appropriate question is: what specific online *behaviors, features, or content* may be associated with benefit or risk to which youth. This is the focus of the most recent work among psychological scientists, yielding some comforting, but also some worrying results.

But first, to understand the role of social media in youths' development, it is necessary to understand the role of social interactions more generally at this critical developmental stage.

APA.ORG APASERVICES.ORG 750 First Street, NE Advocating for APA members and psychology Washington, DC 200

 750 First Street, NE
 202.336.5800

 Washington, DC 20002-4242
 202.336.6123 TDD

⁵ Odgers CL, Jensen MR. Annual Research Review: Adolescent mental health in the digital age: facts, fears, and future directions. J Child Psychol Psychiatry. 2020;61(3):336-348. doi:10.1111/jcpp.13190.



Children's interactions with peers are not merely for fun. It is within the social context that most children's education occurs; thus, peer interactions significantly affect cognitive development. The peer context also is the milieu in which children learn social rules, norms, and expectations; develop emotional competence and morality; and in which all of children's behaviors are consistently reinforced (or corrected), thus influencing long-term behavioral development. Indeed, numerous studies have revealed that children's interactions with peers have enduring effects on their occupational status, salary, relationship success, emotional development, mental health, and even on physical health and mortality over 40 years later ⁶. These effects are stronger than the effects of children's IQ, socioeconomic status, and educational attainment. These enduring effects likely occur because of remarkably powerful and reciprocal interactions between youths' social experiences and their biological development. Children's brains and peripheral nervous systems influence how they interact with peers, and in turn, those experiences change the development of their brain structures, neural pathways, and even how their nervous system responds to stress throughout their lives.

Our brains, our bodies, and our society have been evolving together to shape human development for millennia, influencing our communities, our culture, and our society. Within the last twenty years, the advent of portable technology and social media platforms is changing what took 60,000 years to evolve. We are just beginning to understand how this may impact youth development.

I will first discuss the potential effects of technology and social media use on youth mental health. This will include an outline of five main issues emerging from the research, including the risks of pre-adulthood use of social media, the ramifications that come from unmonitored (and "liked") content online, the potential effects of digital stress, the encouragement of social comparisons, and research demonstrating benefits of social media use among youth. In the

5

 APA.ORG
 State
 <

⁶ For a review, see; Prinstein, M. J., & Giletta, M. (2020). Future Directions in Peer Relations Research. Journal of Clinical Child & Adolescent Psychology, 49(4), 556–572. <u>https://doi.org/10.1080/15374416.2020.1756299</u>.



following section, I will discuss the psychological effects of opportunities lost while youth spend time online. Last, I will discuss potential solutions and policy recommendations.

Online/ Social Media Behaviors and Youth Mental Health

Pre-adulthood use of technology and social media may be particularly concerning. There is reason to be significantly concerned about the age at which many youth begin using technology and social media. Developmental neuroscientists have revealed that there are two highly critical periods for adaptive neural development. Aberrations in our brain growth during these periods may have lifetime implications. One of these is the first year of life. The second begins at the outset of puberty and lasts until early adulthood (i.e., from approximately 10 to 25 years old). This latter period is highly relevant, as this is when a great number of youths are offered relatively unfettered access to devices and unrestricted or unsupervised use of social media and other online platforms ⁷. Within the age range of 10-25 years, change occurs gradually and steadily; thus risks likely are greater towards the beginning of this range and become attenuated as youth mature. Herein, this period is referred to as "pre-adulthood."

At the outset of puberty, adolescents' brains begin developing in a specific, pre-determined sequence. Generally, sub-cortical areas shared with many mammalian species mature before areas at the top layer of the brain, which is responsible for many of our more human capabilities, such as premeditation, reflection, and inhibition. Among these initial areas developing among most youth, typically starting at the ages of 10-12 years old, are regions associated with our craving for "social rewards," such as visibility, attention, and positive feedback from peers. In contrast, regions involved in our ability to inhibit our behavior, and resist temptations (i.e., the prefrontal cortex) do not fully develop until early adulthood (i.e., approximately 10-15 years later). In other words, when it comes to youths' cravings for social attention, they are "all gas pedal with no

6

 APA.ORG

 APASERVICES.ORG
 750 First Street, NE
 202.336.5800

 Advocating for APA members and psychology
 Washington, DC 20002-4242
 202.336.5123 TDD

⁷ Vogels, E. A., Gelles-Watnick, R., & Massarat, N. (2022, August 10). Teens, social media and technology 2022. Pew Research Center. <u>https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/</u>



brakes." Adolescence is thus a developmentally vulnerable period during which youth may be especially motivated to pursue social rewards, and not yet fully capable of restraining themselves.

Research suggests that technology and social media use may exploit this biological vulnerability among youth. Data reveal that social media stimuli, such as receiving "likes" or followers activates the social reward regions of the brain ⁸. In other words, these features of social media capitalize on youths' biologically based need for social rewards before they are able to regulate themselves from over-use. This has at least four significant implications for youth mental health.

Social Media and Loneliness_ Although ostensibly social media platforms are built to foster interpersonal contacts and connections, they are not designed primarily to foster meaningful and mutually rewarding relationships that confer psychological benefits. Relationships are most beneficial to youths' psychological development when they are characterized by support, emotional intimacy, disclosure, positive regard, reliable alliance (e.g., "having each other's backs"), and trust ⁹. It is possible to use social media to foster exactly these types of relationship qualities, such as through direct messaging features. However, these are not the functions that are highlighted on most platforms. More typically, users are directed towards the number of "likes," followers, or reposts they received, often without immediate access to the identity of those who engaged with their profile or content. In other words, platforms are more apt to motivate users towards one's metrics than people themselves, which has led many youth to upload curated or filtered content to portray themselves most favorably. Note that these features of social media, and the resulting behaviors of those who use social media create the exact opposite qualities needed for successful and adaptive relationships (i.e., disingenuous, anonymous, depersonalized). In other

APA.ORG APASERVICES.ORG 750 Advocating for APA members and psychology Was

 750 First Street, NE
 202.336.5800

 Washington, DC 20002-4242
 202.336.6123 TDD

⁸ Sherman, L. E., Hernandez, L. M., Greenfield, P. M., & Dapretto, M. (2018). What the brain 'Likes': neural correlates of providing feedback on social media. Social cognitive and affective neuroscience, 13(7), 699–707. https://doi.org/10.1093/scan/nsv051.

⁹ Furman, W., Bukowski, W. M., Newcomb, A. F., & Hartup, W. W. (1996). The company they keep: Friendship in childhood and adolescence. Cambridge studies in social and emotional development. In W. Bukowski, A. Newcomb & W. Hartup (Eds), The measurement of friendship perceptions: Conceptual and methodological, (41-65).



words, social media offers the "empty calories of social interaction," that appear to help satiate our biological and psychological needs, but do not contain any of the healthy ingredients necessary to reap benefits. Anecdotally, teens' behavior reflects this issue – the "Finsta" phenomenon reflects digital natives' attempt to find more honest and intimate relationships with one another, but without experience in doing so first offline. Scientific data also support this claim; research reveals that in the hours following social media use, teens paradoxically report *increases* rather than decreases in loneliness ¹⁰.

Heightened Risk for Negative Peer Influence. Adolescents frequently are exposed to content online depicting illegal, immoral, dangerous, and unethical behavior. The architecture of many social media platforms allows users to like, repost, or comment on this content. Emerging data suggest that these features of social media present a significant risk to adolescents' mental health. Specifically, data reveal that social media may change adolescents' susceptibility to maladaptive behavior through both biological and psychological pathways. Research examining adolescents' brains while on a simulated social media site, for example, revealed that when exposed to illegal, dangerous imagery, activation of the prefrontal cortex was observed suggesting healthy inhibition towards maladaptive behaviors. However, when these same images were shown with icons indicating that they were "liked" on social media, there was a significant decrease in activation of the brain's imbibition center, suggesting that the "likes" may reduce youths' inhibition (i.e., perhaps increasing their proclivity) towards dangerous and illegal behavior.¹¹ This is evidence that social media features are changing how youths' brains respond to images in ways that confer risk for the development of maladaptive behavior.

APA.ORG APASERVICES.ORG 750 First Street, NE Advocating for APA members and psychology Washington, DC 20

 750 First Street, NE
 202.336.5800

 Washington, DC 20002-4242
 202.336.6123 TDD

 ¹⁰ Armstrong-Carter, E., Garrett, S. L., Nick, E. A., Prinstein, M. J., & Telzer, E. H. (2022). Momentary links between adolescents' social media use and social experiences and motivations: Individual differences by peer susceptibility. Developmental Psychology. Advance online publication. <u>https://doi.org/10.1037/dev0001503</u>.
 ¹¹ See for example, Sherman, L. E., Hernandez, L. M., Greenfield, P. M., & Dapretto, M. (2018). What the brain 'Likes': neural correlates of providing feedback on social media. Social cognitive and affective neuroscience, 13(7), 699–707. <u>https://doi.org/10.1093/scan/nsv051</u>.



There also is evidence that these features of social media may promote a psychological affinity for dangerous and risk-taking behavior. For instance, a study of young high school students revealed that adolescents' exposure to "liked" posts depicting alcohol use was associated with changes in teens' perceptions of their peers' acceptance of alcohol use, which in turn predicted these same teens' early engagement in heavy episodic drinking (i.e., five or more drinks on a single occasion) ¹². Related research has demonstrated that individuals are more likely to "like" a post that they see others have "liked" before them, and this may increase the likelihood of exposure to similarly themed-posts, via AI-derived algorithms ¹³. These findings illustrate clear and powerful ways that the features embedded in social media platforms may have an important and highly concerning effect on youth mental health. Note, it is also possible that these same processes can be used to influence peers towards positive behaviors; however, this has not been adequately investigated.

Risks for Addictive Social Media Use. Youths' biological vulnerabilities also have significant implications for "problematic social media use" or addictive behaviors; note that the regions of the brain activated by social media use overlap considerably with the regions involved in addictions to illegal and dangerous substances ¹⁴. As noted above, the developing brain is built to increase a desire for social rewards (that social media delivers abundantly), without the ability to show the capacities of inhibition and restraint capable among adults. This suggests that youth may be at risk for extraordinarily frequent uses of social media. Several bodies of research reveal that this indeed may be a very significant concern. For instance, data suggest that almost half of

 APA.ORG
 Strend
 Stred
 Stred
 Stred</t

¹² Nesi J, Rothenberg WA, Hussong AM, Jackson KM. Friends' Alcohol-Related Social Networking Site Activity Predicts Escalations in Adolescent Drinking: Mediation by Peer Norms. J Adolesc Health. 2017;60(6):641-647. doi:10.1016/j.jadohealth.2017.01.009.

¹³ Egebark J, Ekström M. Liking what others "Like": using Facebook to identify determinants of conformity. Exp Econ. 2017;21(4):1-22. doi:10.1007/s10683-017-9552-1.

¹⁴ De-Sola Gutiérrez, J., Rodríguez de Fonseca, F., & Rubio, G. (2016). Cell-Phone Addiction: A Review. Frontiers in Psychiatry, 7(175). <u>https://doi.org/10.3389/fpsyt.2016.00175</u>; Griffiths, M. D., Kuss, D. J., & Demetrovics, Z. (2014). Social networking addiction: An overview of preliminary findings. In K. P. Rosenberg & L. Curtiss Feder (Eds.), Behavioral addictions: Criteria, evidence, and treatment (pp. 119–141). Elsevier Academic Press. <u>https://doi.org/10.1016/B978-0-12-407724-9.00006-9</u>; Kirby, B., Dapore, A., Ash, C., Malley, K., & West, R. (2020). Smartphone pathology, agency and reward processing. Lecture Notes in Information Systems and Organisation, 321-329. <u>https://doi.org/10.1007/978-3-030-60073-0_37</u>.



all adolescents report that they use social media "almost constantly" 15. Research also has compared social media use to diagnostic criteria for substance use dependencies, revealing that many adolescents report an inability to stop using social media, even when they want to, remarkable efforts to maintain access to social media, the use of social media to regulate their emotions, a need for increasing social media use to achieve the same level of pleasure (i.e., tolerance symptoms), withdrawal symptoms following abstinence, an significant impairment in their daily educational, social, work routines. A recent study revealed that over 54% of 11-13year-old youth reported at least one of these symptoms of problematic social media use ¹⁶. About 85% of youth report spending more time than intended online and 61% reporting failing when trying to stop or reduce their use of social media 17.

Alterations in Brain Development. Youths' biological vulnerability to technology and social media, and their resulting frequent use of these platforms, also has the potential to alter youths' neural development since our brains develop in response to the environment we live in. Recent studies have revealed that technology and social media use is associated with changes in structural brain development (i.e., changing the size and physical characteristics of the brain). In addition, research with my own colleagues at the University of North Carolina at Chapel Hill recently has revealed that technology and social media use also is associated with changes in how the brain works). Our data has revealed that youth indeed spend a remarkable amount of time using their devices ¹⁸. Objective data measured by teens' phones themselves indicated that the average number of times that youth in sixth grade picked up their phones was over 100, with some interrupting daily activities to pick up their phones over 400 times a day. On average, adolescents

10

APA.ORG APASERVICES.ORG 750 First Street NE 202 336 5800 Advocating for APA members and psychology Washington, DC 20002-4242 202.336.6123 TDD

¹⁵ Vogels, E. A., Gelles-Watnick, R., & Massarat, N. (2022, August 10). Teens, social media and technology 2022. Pew Research Center. https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/ ¹⁶ Boer M, Stevens GWJM, Finkenauer C, van den Eijnden RJJM. The course of problematic social media use in young adolescents: A latent class growth analysis. Child Dev. 2022;93(2):e168-e187. doi:10.1111/cdev.13712 ¹⁷ The Common Sense Census: Media Use by Tweens and Teens. (2021).

https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-

web_0.pdf. ¹⁸ Armstrong-Carter, E., Garrett, S. L., Nick, E. A., Prinstein, M. J., & Telzer, E. H. (2022). Momentary links between adolescents' social media use and social experiences and motivations. Individual differences by peer susceptibility. Developmental psychology.



also reported an average of 8.2 hours of time on their devices each day, with some logging double this amount ¹⁹. The phone "apps" adolescents picked up their devices to use most often were popular social media platforms. Our research using annual fMRI brain scans revealed that more frequent uses of adolescents' devices (i.e., predominantly for social media) was associated with changes in how their brains developed. More phone "pickups" were associated with unique development of brain regions. In short, results found that high social media users may have promoted brain development in a way that may make adolescents more inclined to focus on social rewards (e.g., attention from peers) and altered self-control ²⁰.

Youth's Exposure to Unmonitored Content Poses Potential Risks. There are two domains of problematic content online that many youth are exposed to. Research demonstrates that this also likely contributes to mental health difficulties among children and adolescents. One domain pertains to content that actively showcases and promotes engagement in psychologically disordered behavior, such as sites that discuss eating disordered behaviors (i.e., "pro-Anna" sites that encourage fasting, laxative use, excessive exercise) and pro-cutting sites depicting nonsuicidal self-injury ²¹. Research indicates that this content has proliferated on social media sites, not only depicting these behaviors, but teaching young people how to engage in each, how to conceal these behaviors from adults, actively encouraging users to engage in these behaviors, and socially sanctioning those who express a desire for less risky behavior ²². Moreover, in some cases this content is not removed nor are trigger warnings included to protect vulnerable youth from the effects that exposure to this content can have on their own behavior. This underscores the need for platforms to deploy tools to filter content, display warnings, and create reporting structures to mitigate these harms.

11

 APA.ORG
 State
 <

¹⁹ Maza MT, Fox KA, Kwon S-J, et al. Association of habitual checking behaviors on social media with longitudinal functional brain development. JAMA Pediatr. 2023;177(2):160-167. doi:10.1001/jamapediatrics.2022.4924.
²⁰ See above.

²¹ Lewis, S. P., Heath, N. L., St Denis, J. M., & Noble, R. (2011). The scope of nonsuicidal self-injury on YouTube. Pediatrics, 127(3), e552–e557. <u>https://doi.org/10.1542/peds.2010-2317</u>.

²² Whitlock JL, Powers JL, Eckenrode J. The virtual cutting edge: the internet and adolescent self-injury. Dev Psychol. 2006 May;42(3):407-17. doi: 10.1037/0012-1649.42.3.407. PMID: 16756433.



A second area of concern regarding online content pertains to the frequency of online discrimination and cyberbullying, including youths' posts that encourage their peers to attempt suicide. Research demonstrates that online victimization, harassment, and discrimination against racial, ethnic, gender, and sexual minorities is frequent online and often targeted at young people ²³. LGBTQ+ youth experience a heightened level of bullying, threats, and self-harm on social media. One in three young LGBTQ+ people have said that they had been sexually harassed online, four times as often as other young people ²⁴. Brain scans of adults and youths reveal that online harassment activates the same regions of the brain that respond to physical pain and trigger a cascade of reactions that replicate physical assault and create physical and mental health damage ²⁵. Moreover, research has revealed that online discrimination often is harsher and more severe than offline discriminatory experiences. Results reveal that the effects of online discrimination and bullying on youths' risk for depression and anxiety are significant above and beyond the effects of experiences that these same youth experience offline. The permanence, potential for worldwide dissemination, anonymity, and the like, repost, and comment features afforded on most social media platforms seem to contribute to youths' mental health difficulties. As with other forms of harassment and associated harms, new policies and processes are needed to blunt the impact of these harms.

The Potential Effects of Digital Stress. Social media platforms frequently include a variety of features designed to maintain users' engagement online, or encourage users to return to the app. Psychological theory and research have begun to reveal that this has become a significant source

12

 APA.ORG
 State
 <

²³ Moreno, M. A., Chassiakos, Y. R., Cross, C., Hill, D., Ameenuddin, N., Radesky, J., Hutchinson, J., Boyd, R., Mendelson, R., Smith, J., Swanson, W. S., & Media, C. C. (2016). Media use in school-aged children and adolescents. Pediatrics, 138(5). https://doi.org/10.1542/peds.2016-2592; Tynes, B. M., Giang, M. T., Williams, D

R., & Thompson, G. N. (2008). Online racial discrimination and psychological adjustment among adolescents. Journal of Adolescent Health, 43(6), 565-569. <u>https://doi.org/10.1016/j.jadohealth.2008.08.021</u>.

²⁴ Out Online: The Experiences of LGBT Youth on the Internet. (2013). GLSEN. https://www.glsen.org/news/outonline-experiences-lgbt-youth-internet.

²⁵ Cannon, D. S., Tiffany, S. T., Coon, H., Scholand, M. B., McMahon, W. M., & Leppert, M. F. (2007). The PHQ-9 as a brief assessment of lifetime major depression. Psychological Assessment, 19(2), 247-251. <u>https://doi.org/10.1037/1040-3590.19.2.247</u>.



of stress. This is highly relevant since stress is one of the strongest predictors of children's and adolescents' mental health difficulties, including suicidal behavior. "Digital stress," is characterized by a youth's a) connection overload (i.e., notification and implicit social requirements to participate on social media platforms), b) the fear of missing out on conversations and other social interactions taking place exclusively online, c) the need to remain constantly available to others online, and d) approval anxiety (i.e., concerns about the response to one's own posts) are each notable factors influencing the way youth think about their connection to online platforms ²⁶. Nearly half of all young people participating in online platforms report experiencing digital stress. Research demonstrates that higher levels of digital stress are associated with greater increases in depressive symptoms among adolescents 27.

Social Media Encourages Social Comparisons. The quantitative nature of social media, combined with the use of visual stimuli, creates a fertile ground for social comparisons. Adolescence, a period defined by psychologists as a process of identity development via reflected appraisal processes (i.e., evaluating oneself based on feedback from peers) are especially likely to engage with social media in ways that allow them to compare their appearance, friends, social activities with others with what they see online, especially when those in their own social network are commenting and "liking" these same posts. The opportunity for constant feedback, commentary, quantitative metrics of approval, and 24-hour social engagement is unprecedented among our species. Research suggests that these social comparison processes, and youths' tendency to seek positive feedback or status (i.e., more "likes," followers, online praise) is associated with a risk for depressive symptoms ²⁸. In addition, psychological science demonstrates

202.336.5800

APA.ORG APASERVICES.ORG 750 First Street, NE Advocating for APA members and psychology Washington, DC 20002-4242 202.336.6123 TDD

²⁶ Steele, R. G., Hall, J. A., & Christofferson, J. L. (2020). Conceptualizing Digital Stress in Adolescents and Young Adults: Toward the Development of an Empirically Based Model. Clinical child and family psychology review, 23(1), 15-26. https://doi.org/10.1007/s10567-019-00300-5

²⁷ Nick, E. A., Kilic, Z., Nesi, J., Telzer, E. H., Lindquist, K. A., & Prinstein, M. J. (2022). Adolescent Digital Stress: Frequencies, Correlates, and Longitudinal Association With Depressive Symptoms. The Journal of adolescent health : official publication of the Society for Adolescent Medicine, 70(2), 336-339 https://doi.org/10.1016/j.jadohealth.2021.08.025.
 ²⁸ Choukas-Bradley, S., Nesi, J., Widman, L., & Galla, B. M. (2020). The Appearance-Related Social Media

Consciousness Scale: Development and validation with adolescents. Body Image, 33, 164-174.



that exposure to this online content is associated with lower self-image and distorted body perceptions among young people. This exposure creates strong risk factors for eating disorders, unhealthy weight-management behaviors, and depression ²⁹. As with other impacts of online platforms, evidence indicates that these body image issues are particularly prevalent in LGBTQ+ youth. Leaving these youth more predisposed to eating disorders, depression, bullying, substance abuse and other mental health harms.

Potentially Beneficial Effects of Social Media Use. It is important to acknowledge that research on social media use and adolescent development is relatively new, as are many social media platforms. In addition, there has been remarkably little funding designated for research on this topic. Consequently, the long-term effects of social media use on youth development is relatively uncharted. For instance, above I discussed some of the potential effects of technology social media use on brain development. Yet, it is unknown whether adolescent brain development, known for its plasticity, may "correct" some of the alternations in brain structure or function, whether compensatory neural processes may develop, or whether these alterations may confer unknown future strengths.

In addition, there is some research demonstrating that social media use is linked with positive outcomes that may benefit psychological development among youth. Perhaps most notably, psychological research suggests that young people form and maintain friendships online. These relationships often afford opportunities to interact with a more diverse peer group than offline, and the relationships are close and meaningful and provide important support to youth in

https://doi.org/10.1016/i.bodyim.2020.02.017; Hawes, T., Zimmer-Gembeck, M. J., & Campbell, S. M. (2020). Unique associations of social media use and online appearance preoccupation with depression, anxiety, and appearance rejection sensitivity. Body Image, 33, 66-76. https://doi.org/10.1016/j.bodyim.2020.02.010; Nesi, J.L., & Prinstein, M.J. (2015). Using social media for social comparison and feedback seeking: Gender and popularity moderate associations with depressive symptoms. Journal of Abnormal Child Psychology, 43(8), 1427–1438. ²⁹ Carrotte, E. R., Vella, A. M., & Lim, M. S. (2015). Predictors of "liking" three types of health and fitness-related content on social media: A cross-sectional study. Journal of Medical Internet Research, 17(8), e205. https://doi.org/10.2196/jmir.4803; https://doi.org/10.1016/j.paid.2011.11.011.

14

 APA.ORG
 State
 <



times of stress ³⁰. The buffering effects of social support from peers has been well documented in the psychological literature ³¹. This may be especially important for youth with marginalized identities, including racial, ethnic, sexual, and gender minorities. Digital platforms provide an important space for self-discovery and expression for LGBTQ+ youth.

Research also suggests that during the COVID-19 lockdown from 2020-2021, the use of one-on-one (i.e., direct messaging) on social media and sharing funny content reduced stress among youth. There also is some evidence that youth are more likely to engage in civic activism online than off ³².

A growing area of research has also focused on the use of youths' interest in online activities as an opportunity for digital-based intervention ³³. Adolescents report high levels of comfort with, and a preference for, online communication, especially when discussing mental health. Studies also show that adolescents commonly use the internet for mental health information ³⁴.

15

APA.ORG APASERVICES.ORG

 ArAsservices.org
 750 First Street, NE
 202.336.5800

 Advocating for APA members and psychology
 Washington, DC 20002-4242
 202.336.6123 TDD

³⁰Anderson, M., & Jiang, J. (2018, November 28). 2. Teens, friendships and online groups. Pew Research Center: Internet, Science & Tech; Pew Research Center: Internet, Science & Tech.

https://www.pewresearch.org/internet/2018/11/28/teens-friendships-and-online-groups/; Charmaraman L, Hodes R, Richer AM. Young Sexual Minority Adolescent Experiences of Self-expression and Isolation on Social Media: Cross-sectional Survey Study. JMIR Ment Health. 2021;8(9):e26207. doi:10.2196/26207; Massing-Schaffer M, Nesi J, Telzer EH, Lindquist KA, Prinstein MJ. Adolescent Peer Experiences and Prospective Suicidal Ideation: The Protective Role of Online-Only Friendships. J Clin Child Adolesc Psychol. 2022;51(1):49-60. doi:10.1080/15374416.2020.1750019; Marciano L, Ostroumova M, Schulz PJ, Camerini A-L. Digital Media Use and Adolescents' Mental Health During the Covid-19 Pandemic: A Systematic Review and Meta-Analysis. Front

Public Health. 2021;9:793868. doi:10.3389/fpubh.2021.793868; Baskin-Sommers A, Simmons C, Conley M, et al. Adolescent civic engagement: Lessons from Black Lives Matter. Proc Natl Acad Sci USA. 2021;118(41). doi:10.1073/pnas.2109860118.

³¹ Cohen, S., & Wills, T. A. (1985). Stress, social support, and the buffering hypothesis. Psychological Bulletin, 98(2), 310–357. <u>https://doi.org/10.1037/0033-2909.98.2.310</u>.

³² Marciano, L., Ostroumova, M., Schulz, P. J., & Camerini, A. L. (2022). Digital Media Use and Adolescents' Mental Health During the Covid-19 Pandemic: A Systematic Review and Meta-Analysis. Frontiers in public health, 9, 793868. <u>https://doi.org/10.3389/fpubh.2021.793868</u>.

 ³³ Bradford, S., & Rickwood, D. (2015). Young people's views on electronic mental health assessment: Prefer to type than talk? Journal of Child and Family Studies, 24(5), 1213–1221. https://doi.org/10.1007/s10826-014-9929-0.34
 ³⁴ Intervention and Prevention in the Digital Age. (2022). In J. Nesi, E. Telzer, & M. Prinstein (Eds.), Handbook of Adolescent Digital Media Use and Mental Health (pp. 363-416). Cambridge: Cambridge University Press. doi:10.1017/9781108976237.019; Park, E., & Kwon, M. (2018). Health-Related Internet Use by Children and Adolescents: Systematic Review. Journal of medical Internet research, 20(4), e120. https://doi.org/10.2196/jmir.7731.



These elements, taken together, present the possibility that digital modes of treatment and other health interventions may be particularly effective for young people.

Research into the field of digital mental health interventions is growing and the existing information is heavily skewed toward more established modalities (e.g., telehealth, online/webbased interventions). Evidence supports the use of videoconferencing as an effective form of treatment for youth mental health across a range of problems ³⁵. While many computerized programs and internet-based treatment programs were found to be of moderate to high quality, a systematic review of the literature found that the inclusion of a therapist or clinician improved outcomes in adolescents with depression and anxiety over those that were self-paced ³⁶. Young people with a history of suicidal ideation often prefer to initially seek and receive healthcare online ³⁷. Even when individuals have strong support systems offline, they may struggle to access that support in times of need ³⁸. Early indications that online support may be appealing because of its immediate nature and because the interactions are among peers with shared experience and

16

 APA.ORG
 State
 <

³⁵ Myers, K. M., Valentine, J. M., Melzer, S. M. (2007, Nov). Feasibility, acceptability, and sustainability of telepsychiatry for children and adolescents. Psychiatric Services, 58(11), 1493-1496. <u>https://doi.org/10.1176/ps.2007.58.11.1493</u>; Nelson, E. L., Cain, S., & Sharp, S. (2017, Jan). Considerations for

antps://doi.org/10.1176/ps.2007.58.11.1495; Nelson, E. L., Calit, S., & Sharp, S. (2017, Jan). Considerations for conducting telemental health with children and adolescents. Child Adolescent Psychiatric Clinics of North America, 26(1), 77-91. <u>https://doi.org/10.1016/j.chc.2016.07.008</u>.
 ³⁶ Clarke, T. C., Black, L. I., Stussman, B. J., Barnes, P. M., & Nahin, R. L. (2015). Trends in the use of

Clarke, I. C., Black, L. I., Stussman, B. J., Barnes, P. M., & Nahn, R. L. (2015). Trends in the use of complementary health approaches among adults: United States, 2002-2012. National health statistics reports, (79), 1–16.; Wozney L, McGrath P, Gehring N, Bennett K, Huguet A, Hartling L, Dyson M, Soleimani A, Newton A. eMental Healthcare Technologies for Anxiety and Depression in Childhood and Adolescence: Systematic Review of Studies Reporting Implementation Outcomes. JMIR Ment Health 2018;5(2):e48. https://mental.jmir.org/2018/2/e48; Hollis, C., Falconer, C. J., Martin, J. L., Whittington, C., Stockton, S., Glazebrook, C., & Davies, E. B. (2017). Annual Research Review: Digital health interventions for children and young people with mental health problems - a systematic and meta-review. Journal of child psychology and psychiatry, and allied disciplines, 58(4), 474–503. https://doi.org/10.1111/jcpp.12663.

 ³⁷ Frost, M., Casey, L. M., & O'Gorman, J. G. (2017). Self-injury in young people and the help-negation effect.
 Psychiatry Research, 250, 291–296. <u>https://doi.org/10.1016/j.psychres.2016.12.022</u>.
 ³⁸ Kruzan, K. P., Whitlock, J., & Bazarova, N. N. (2021). Examining the Relationship Between the Use of a Mobile

Peer-Support App and Self-Injury Outcomes: Longitudinal Mixed Methods Study. JMIR Mental Health, 8(1), e21854. <u>https://doi.org/10.2196/21854</u>; Lavis, A., & Winter, R. (2020). #Online harms or benefits? An ethnographic analysis of the positives and negatives of peer-support around self-harm on social media. Journal of Child Psychology and Psychiatry, and Allied Disciplines, 61(8). <u>https://doi.org/10.1111/jcpp.13245</u>.



experiential knowledge ³⁹. Yet, it is crucial for young people to have access to in-person screenings and clinician support.

Psychological Effects of Lost Opportunities While Youth Are Online

Every hour youth spend online is an hour that is not being spent on alternative ("in real life") activities. In some cases, this may protect adolescents' exposure to peer contexts in which substance use and sexually risky behaviors occur. However, youths' online activities also may preclude engagement in activities necessary for successful maturation and psychological adaptation. Perhaps most concerning is the extent to which research has demonstrated that technology and social media use is interfering with youths' sleep.

Research has supported the link between technology use and sleep in several ways. Perhaps most compelling are data from meta-analyses (i.e., a statistical integration of findings from across an entire body of research) indicating that 60% of adolescents report using technology in the hour before bedtime, and more screen time is associated with poorer sleep health and failure to meet sleep duration requirements set by the American Academy of Sleep Medicine, partly due to delayed melatonin release, delayed bedtimes, and increases in overstimulation and difficulty disengaging from online social interactions. Interventions to reduce nighttime screen use are successful in increasing sleep duration ⁴⁰.

This has critical implications for adolescent development. Research suggests that insufficient sleep is associated with poor school performance, difficulties with attention, stress

17

 APA.ORG

 APASERVICES.ORG
 750 First Street. NE
 202.336.5800

 Advocating for APA members and psychology
 Washington, DC 20002-4242
 202.336.6123 TDD

³⁹ Marchant, A., Hawton, K., Stewart, A., Montgomery, P., Singaravelu, V., Lloyd, K., Purdy, N., Daine, K., & John, A. (2017). A systematic review of the relationship between internet use, self-harm and suicidal behaviour in young people: The good, the bad and the unknown. PLOS ONE, 12(8), e0181722. https://doi.org/10.1371/journal.pone.0181722; Thoits, P. A. (2011). Mechanisms Linking Social Ties and Support

https://doi.org/10.1371/journal.pone.0181722;
 Thoits, P. A. (2011). Mechanisms Linking Social Ties and Support to Physical and Mental Health. Journal of Health and Social Behavior, 52(2), 145–161.
 https://doi.org/10.1177/0022146510395592.
 ⁴⁰ Telzer EH, Goldenberg D, Fuligni AJ, Lieberman MD, Gálvan A. Sleep variability in adolescence is associated

⁴⁰ Telzer EH, Goldenberg D, Fuligni AJ, Lieberman MD, Gálvan A. Sleep variability in adolescence is associated with altered brain development. Dev Cogn Neurosci. 2015;14:16-22. doi:10.1016/j.dcn.2015.05.007.



regulation, and increased risk for automobile accidents. Neuroscientific research has demonstrated that inconsistent sleep schedules are associated with changes in structural brain development in adolescent years. In other words, youths' preoccupation with technology and social media may deleteriously affect the size of their brains ⁴¹.

In addition, note that youth also engage with online and social media apps *while participating* in other activities. Indeed, early studies show that when youth are engaging in schoolwork, they often are doing so alongside the use of social media platforms, a phenomenon called "media multitasking" ⁴². Research clearly demonstrates that most humans cannot multitask, but rather are rapidly task-shifting – a process associated with poorer memory and comprehension among youth ⁴³. Evidence shows that these phenomena only worsen with heavier use of social media, with more common symptoms such as mind wandering and higher levels of impulsivity among young adults who use social media more frequently ⁴⁴.

Potential Solutions and Policy Implications

 APA.org

 APASERVICES.org
 750 First Street, NE
 202.336.5800

 Advocating for APA members and psychology
 Washington, DC 20002-4242
 202.336.6123 TDD

⁴¹ Achterberg M, Becht A, van der Cruijsen R, et al. Longitudinal associations between social media use, mental well-being and structural brain development across adolescence. Dev Cogn Neurosci. 2022;54:101088. doi:10.1016/j.dcn.2022.101088.

⁴² Jeong, S.-H., & Hwang, Y. (2012). Does Multitasking Increase or Decrease Persuasion? Effects of Multitasking on Comprehension and Counterarguing. Journal of Communication, 62(4), 571–587. <u>https://doi.org/10.1111/j.1460-2466.2012.01659.x</u>; van der Schuur, W. A., Baumgartner, S. E., Sumter, S. R., & Valkenburg, P. M. (2015). The consequences of media multitasking for youth: A review. Computers in Human Behavior, 53, 204–215. <u>https://doi.org/10.1016/j.chb.2015.06.035</u>; L. Mark Carrier, Larry D. Rosen, Nancy A. Cheever, Alex F. Lim, Causes, effects, and practicalities of everyday multitasking, Developmental Review (2015), doi: 10.1016/j.dr.2014.12.005.

⁴³ Ralph, B. C., Thomson, D. R., Cheyne, J. A., & Smilek, D. (2014). Media multitasking and failures of attention in everyday life. Psychological research, 78(5), 661–669. <u>https://doi.org/10.1007/s00426-013-0523-7</u>.

⁴⁴ Ophir, E., Nass, C., & Wagner, A. D. (2009). Cognitive control in media multitaskers. Proceedings of the National Academy of Sciences of the United States of America, 106(37), 15583–15587.

https://doi.org/10.1073/pnas.0903620106; Ralph, B. C., Thomson, D. R., Cheyne, J. A., & Smilek, D. (2014). Media multitasking and failures of attention in everyday life. Psychological research, 78(5), 661–669.

https://doi.org/10.1007/s00426-013-0523-7; Baumgartner, S. E., Weeda, W. D., van der Heijden, L. L., & Huizinga, M. (2014). The Relationship Between Media Multitasking and Executive Function in Early Adolescents. The Journal of Early Adolescence, 34(8), 1120–1144. <u>https://doi.org/10.1177/0272431614523133</u>; Baumgartner, Susanne & van der Schuur, Winneke & Lemmens, Jeroen & te Poel, Fam. (2018). The Relationship Between Media Multitasking and Attention Problems in Adolescents: Results of Two Longitudinal Studies. Human Communication Research. 44, 3-30. 10.1093/hcre.12111.



The internet and the introduction of social media platforms have literally changed our species through new forms of social interaction, new rules for discourse, the rapid spread of information, and concomitant changes in the types of relationships that previously had defined the human race for millennia. This is an extraordinarily high priority area for additional scientific research; however, this work has been woefully underfunded. Currently, federal agencies lack both the direction, expertise, and dedicated funding to adequately research both the positive and negative impacts of online platforms. Tech companies responsible for these platforms employ dozens of researchers focused on designing products and observing how users engage with them. The federal government must match or exceed this commitment to ensure the public has an adequate understanding of how these platforms work and how users, especially children, are using these platforms and their impact. The research that is needed should be longitudinal to allow for long-term follow-up. Research should capture the experience of diverse samples, utilize the benefits of technology to capture objective measures of behavior, include technology (e.g., fMRI) to study biopsychosocial effects, and importantly, should make use of the data available to social media companies to fully understand the effects of social media and protect the common good. This effort must be paired with required increases in transparency and access to data for researchers to further understand online activity. New transparency and reporting requirements should ensure user privacy, while creating new mechanisms for researchers and policymakers to understand how these online spaces operate.

Recently, Congress allocated \$15M to research on social media and adolescent mental health. This is appreciated, yet barely sufficient to fund more than 3-5 individual studies that would meet the abovementioned specifications. At least \$100M in funds will be needed to reflect a serious commitment to this research area across federal agencies. And, as we are on the precipice of a new digital age with artificial intelligence (AI) and machine learning directly impacting us across the lifespan, it is paramount that our country invest in research to protect future generations.

APA.ORG APASERVICES.ORG 750 First Street, NE Advocating for APA members and psychology Washington, DC 20

 750 First Street, NE
 202.336.5800

 Washington, DC 20002-4242
 202.336.6123 TDD



Such research also might address the role of social media algorithms on users' experience. This requires access to data for independent researchers to understand how algorithms work ⁴⁵. Social media companies employing algorithms to display content to users should take steps to provide explanations on how these technologies work and how they might drive or reward certain types of posts or behavior. Data from algorithms, along with internal research, should also be made public to allow researchers and policymakers to achieve a greater understanding of the impacts of social media on users, particularly children. Federal agencies should prioritize research into the impacts of social media and provide private researchers with grants and other support to ensure findings relating to these platforms are made broadly available.

There is much more Congress and federal agencies can do to provide education around how best to use online platforms to mitigate harmful impacts. A coalition of more than 150 organizations, led by APA, have called on the Surgeon General to create and distribute resources dedicated to teaching children and caregivers about online social media use ⁴⁶. There is a clear need for an education campaign that enhances the public's understanding of the potential harms posed by social media and encourages caregivers and children to educate themselves with evidence-informed suggestions for its appropriate use. At the same time, it is important to acknowledge social media's potential to provide children with a healthy space for convening and companionship. While we recognize the need for additional research in this area, the very real harms of social media are impacting our children today, and more must be done to communicate and mitigate the impacts of online social media use. Educating young users and their caregivers about how best to use the platforms to mitigate negative impacts is an essential intervention that can start today. A public education campaign should include information about the specific dangers social media poses to adolescents, how parents and caregivers can best navigate learning

20

APA.ORG APASERVICES.ORG 750 First Street, NE 202.336.5800 Advocating for APA members and psychology Washington, DC 20002-4242 202.336.6123 TDD

⁴⁵ Epps-Darling, A., Bouyer, R. T., & Cramer, H. (2020, October). Artist gender representation in music streaming. In Proceedings of the 21st International Society for Music Information Retrieval Conference (Montréal, Canada) (ISMIR 2020). ISMIR (pp. 248-254); Bravo, D. Y., Jefferies, J., Epps, A., & Hill, N. E. (2019). When things go viral: Youth's discrimination exposure in the world of social media. In Handbook of Children and Prejudice (pp. 269-287). Springer, Cham. <u>https://doi.org/10.1007/978-3-030-12228-7_15</u>.
 ⁴⁶ (2023). Apaservices.org. https://www.apaservices.org/advocacy/news/surgeon-general-dangers-social-media



more about these dangers, how best to communicate the risks with their children, and ultimately how to educate their children on the best methods for using social media in a safe way.

APA also advocates for Congress and federal agencies to require social media companies to do more to combat this issue. <u>Platforms can create and provide new tools aimed at mitigating the harms associated with platform use</u>. Requiring social media companies to provide children and their caregivers with options to make changes to their social media settings can promote mental health by protecting their information, disabling features that are particularly addictive, and opting out of algorithm processes that serve up problematic or harmful content. Social media companies can also be required to set defaults to address harms to young users.

Warnings on harmful content should also be considered to reduce exposure of young people to content that may negatively impact their mental health or well-being and companies should be held accountable for the proliferation of this content. Social medial companies should acknowledge known impacts of their platforms, providing warnings and resources to parents and caregivers of young users, develop plans to mitigate known harms, and determine whether these warnings and plans were effective, with iterative updates based on these findings. Social media platforms must work to prevent and mitigate harmful content, such as promotion of self-harm, suicide, eating disorders, substance use and sexual exploitation. Independent audits can assess risks and determine whether platforms are taking meaningful steps to prevent damage and these must be paired with enforcement actions and accountability mechanisms for when platforms fail to effectively mitigate harms to children.

As discussed throughout this testimony, more must be done to specifically protect those children belonging to traditionally marginalized and minoritized communities. Mental health and other harms can disproportionately fall on LGBTQ+ youth, and resources should be dedicated to ensuring a reduction in these harms. More must be required of platforms to discourage and prevent cyberbullying and other forms of online hate and discrimination. <u>Reporting structures should be</u>

 APA.ORG

 APASERVICES.ORG
 750 First Street, NE
 202.336.5800

 Advocating for APA members and psychology
 Washington, DC 20002-4242
 202.336.6123 TDD

123



more robust to allow for instances to be tracked and discouraged. Reforms to platform user experience should be prioritized to ensure members of these communities are protected from disproportionate harm.

Specific legislation has been proposed across the federal government that would take productive steps in mitigating the known negative impacts of social media. The Kids Online Safety Act (KOSA) is one such piece of legislation. In 2022, APA CEO Arthur C. Evans Jr., PhD, said, "The Kids Online Safety Act is an important first step in reining in the harms caused to children by social media platforms," and "enacting measures that curtail harmful practices while authorizing research to understand additional impacts is a thoughtful strategy"⁴⁷. KOSA and other previously proposed legislative fixes such as updates to the Children Online Privacy and Protection Act represent important steps by Congress and I encourage their debate and adoption.

APA is heartened by the focus on mental health in Congress, and eager to work with this committee and its members to develop legislation and enact the bills cited above. Your actions now can make all the difference in how our young people interact with and are impacted by online spaces. Together, psychology, other scientific disciplines, parents, caregivers, teachers, tech companies, and policymakers can work to solve this serious problem. APA is a ready partner and looks forward to working with the committee to put in place critical changes to our current system that improve the lives of our children and the flourishing of online spaces.

APA.ORG APASERVICES.ORG 750 First Street, NE Advocating for APA members and psychology Washington, DC 200

 750 First Street, NE
 202.336.5800

 Washington, DC 20002-4242
 202.336.6123 TDD

^{47 (2023).} Apaservices.org. https://www.apaservices.org/advocacy/news/kids-online-safety-legislation

Senator Sheldon Whitehouse Senate Judiciary Committee Hearing "Protecting Our Children Online" Questions for the Record for Kristin Bride Submitted February 21, 2023

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

Senator Sheldon Whitehouse Senate Judiciary Committee Hearing "Protecting Our Children Online" Questions for the Record for Michelle C. DeLaune Submitted February 21, 2023

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

<u>Questions from Senator Tillis for Michelle</u> <u>DeLaune, President and CEO of National Center</u> <u>for Missing & Exploited Children (NCMEC)</u>

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

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

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

Senator Sheldon Whitehouse Senate Judiciary Committee Hearing "Protecting Our Children Online" Questions for the Record for Josh Golin Submitted February 21, 2023

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

<u>Questions from Senator Tillis for Josh Golin,</u> <u>Executive Director of Fair Play</u>

1. What are the largest impacts of high screen time for children? How can this be mitigated?

2. You've raised concern in the past that even EdTech (Educational Technology), in terms of high screen time, can be dangerous for our children. Do you see a path forward where a balance can be struck with EdTech as it does have it benefits in certain situations?

2. What is surveillance advertisement and how is this particularly detrimental to children? How can this be mitigated?

3.Beyond surveillance advertisement, are there any other algorithmic-based practices being implemented that are particularly detrimental to children? How can this be mitigated?

130

4. Are you aware of any surveillance advertisements or algorithms that are used to target children, specifically to promote drugs and the sale of narcotics?

Senator Sheldon Whitehouse Senate Judiciary Committee Hearing "Protecting Our Children Online" Questions for the Record for Emma Lembke Submitted February 21, 2023

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

Senator Sheldon Whitehouse Senate Judiciary Committee Hearing "Protecting Our Children Online" Questions for the Record for John Pizzuro Submitted February 21, 2023

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

Judiciary Committee Hearing: Protecting Our Children Online February 14, 2023 Questions for the Record Senator Peter Welch

Questions for Mr. John Pizzuro

Big tech companies are exacerbating the fentanyl crisis—they've turned a blind eye to folks selling drugs on their platforms, giving dealers an easy way to reach buyers online. That's a particular problem for our kids, who can easily buy dangerous drugs through social media platforms.

- 1. When you served in the New Jersey State Police Department, what challenges did you or your colleagues face in preventing, identifying, and catching these transactions on social media?
- 2. What steps should Congress take to make it harder for people to market drugs to kids online?

<u>Questions from Senator Tillis for John Pizzuro,</u> <u>CEO of Raven</u>

1. As you know, in 2021, the National Center for Missing and Exploited Children (NCMEC) cyber tipline received 29 million reports of suspected online child sexual exploitation- child sexual abuse material (CSAM). In your experience how long does it take to review each cyber tipline report?

2. Are there certain States that are receiving a higher volume of cyber tipline reports than others? If so, why are their volumes higher?

3. What resources and tools do our law enforcement need to efficiently and effectively review the cyber tipline reports?

Senator Sheldon Whitehouse Senate Judiciary Committee Hearing "Protecting Our Children Online" Questions for the Record for Mitch J. Prinstein Submitted February 21, 2023

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

Judiciary Committee Hearing: Protecting Our Children Online February 14, 2023 Questions for the Record Senator Peter Welch

<u>Questions for Dr. Mitch Prinstein</u> In addition to using personal devices at home, many children have access to technology in classrooms and use devices as part of standard lessons.

- 1. What research exists regarding how the use of technology in the classroom either positively or negatively affects students' mental health, physical health, learning outcomes, and behavior?
- 2. How should educational institutions consider this research when making decisions regarding technology use in classrooms?

EISENBERG @ BAUM, LLP

February 21, 2023

Re: Briefing in Response to February 14, 2023 United States Senate Committee on the Judiciary Hearing on Protecting our Children Online

Dear Senators,

We represent Kristin Bride, the parent of 16-year-old Carson Bride, who was viciously bullied on anonymous apps before taking his own life. Kristin Bride brought a national class action against Snap Inc. and two anonymous apps YOLO and LMK for their defective product designs and false product misrepresentation. The lawsuit was dismissed in the Central District Court of California on January 10, 2023, citing Section 230 immunity.

We also represent individuals and entities such as:

- Tyler Clementi Foundation and other individual families advocating against cyberbullying
- three young children and their families and a nationwide class who were victims of
 physically rape, sexually grooming, and sextorted for CSAM production,
- Children and/or families who lost their lives due to illicit drug sale in a nationwide class
 action
- Children and/or families who lost the lives due to the choking challenge in a nationwide class action

At the senate judiciary committee's hearing, Kristin Bride explained that the lawsuit was not about content of third parties but focused on the designs of apps which make anonymity the integral feature. Anonymous messaging apps – predecessors of YOLO and LMK – distributed among teens had historically led to numerous reports of suicide. Many senators at the hearing responded to Ms. Bride's testimony, reiterating the compelling need for reforms to Section 230. The Committee also requested that Ms. Bride submit proposals or requests for how Section 230 should be reformed.

Section 230 of the Communications Decency Act is in critical need of reform. In its present form, Section 230 enables powerful tech companies to escape any and all liability for their involvement in discrimination, harassment, and human rights abuses. To address the failures of Section 230 in allowing rampant harms to be inflicted upon users—many of whom are children—we propose the following reforms to this Committee: (1) Section 230 immunity should only be applicable in cases where defendants can demonstrate effective mechanisms for combatting illegal and harmful content on their platform; (2) Section 230 immunity should be treated as an affirmative defense, necessitating defendants to bear the burden of proof and permitting plaintiffs to obtain an appropriate scope of discovery; (3) Section 230 immunity should *not* be applicable to a defendant's own representations, recommendation algorithms, and other flawed product

EISENBERG & BAUM, LLP 24 UNION SQUARE EAST - PENTHOUSE NEW YORK NY 10003 PH 212 353 8700 FAX 917 591 2875 EandBLaw.com

EISENBERG @ BAUM, LLP

designs; and, (4) Section 230 should expressly permit litigants to calculate damages through defendant companies' data revenue.

1. Section 230 should apply only where companies can demonstrate that they have established protocols to safeguard users expeditiously and meaningfully from illegal and harmful content on their platforms.

Section 230, as currently written, is used as a get-out-of-litigation-free card by tech platforms to hide from liability. In reforming Section 230, we ask this Committee to gain insight from examples of other safe harbor laws applicable to technology companies that are harmonized to protect both tech platforms and users.

For example, Congress created the DMCA Safe Harbor provisions under 17 U.S.C. §512 which require that Online Service Providers (OSPs) demonstrate eligibility for a safe-harbor in order to limit exposure to liability for copyright violations on contents hosted on their platforms. Pursuant to the DMCA, OSPs seeking protection under 17 U.S.C. §512 must expeditiously remove or take down the alleged copyright-infringing material of which it is notified. This process allows for a counter-notification process so that both users are able to make use of the OSP's process. It must designate agents to receive such copyright-infringing notices from users and must take action upon actual or constructive knowledge. OSPs are also required to establish a process of identifying and sanctioning repeat offenders that infringe copyrights.

Like the above, that Section 230 immunity should also be revised so that immunity is not freely provided as a blanket protection. Instead, social media platforms must be able to demonstrate that they have protocols and the capacity to remove and block access to harmful and illegal content that it is notified of, expeditiously and meaningfully.

2. Section 230 should be used as an affirmative defense: defendants raising the affirmative defense must bear the burden of proof, and plaintiffs should be entitled to an appropriate scope of discovery.

We propose that the Committee refashion Section 230 as an affirmative defense, not as a blanket immunity. Under this framework, tech companies would bear the burden of proof to show that they implemented effective, available technology to screen out harmful content relevant to the demographics of their users that the tech platforms knew or should have known about. Since defendant tech companies would bear the burden of proof in asserting the affirmative defense, plaintiffs should be entitled to an appropriate scope of discovery in the early stages of litigation surrounding the affirmative defense raised.

Currently, plaintiffs, courts, consumers, and other members of the public face a Blackbox when it comes to the operations and safety protocols that tech companies purport to employ. As drafted, Section 230 immunity has been interpreted by courts to dismiss claims at the earliest stage of litigation, plaintiffs' claims – even where they allege the most atrocious harms occurring on a routine basis to the most vulnerable population in America.

EISENBERG @ BAUM, LLP

Whistleblowers like Frances Haugen have brought to light that technology products are designed to maximize profit to companies at the cost of known harms to children. However, without an appropriate scope of discovery, the public is provided with no information about the safety of the tech products, and courts can only "take the defendants' words for it." Because all of the relevant information about the designs of the products and safety concerns are under exclusive control of the tech platforms, the platforms must bear the burden to produce the evidence in order to use Section 230 as a defense, and plaintiffs must be able to probe into evidence to counter it.

3. Section 230 Should Not Apply to Tech Companies' Own Representations, Recommendation Algorithms, and Other Dangerously Designed Products.

We recognize that the elephant in the room in these discussions surround Section 230's potential implications upon free speech. However, creating a law that upholds consumers' right to be redressed for harms caused by tech companies' own representations and product designs is an issue that is analytically distinct from free speech and censorship issues. As cogently written by Hon. Judge Hawkins and attorney M. Stanford in the University of Chicago Law Review¹:

"... Sure, threatening the immunity of purportedly biased platforms offers a potent political cudgel. But in a strictly legal sense, they are two different issues. One is whether (and if so, to what degree) absolute immunity under Section 230 has outlived its usefulness, which we assess by weighing the political, economic, and social costs of various approaches to platform liability for unlawful user behavior. The other concerns platforms' considerable power over speech in what people might consider today's public square. While one might ultimately prove useful in coaxing platforms to address the other, the censorship debate's preoccupation with platforms' removal of allegedly harmful but otherwise lawful content asks a separate question—namely, has the time come to require platforms to provide users the same free speech protections that Congress must afford the protestors on its front steps? Modernizing Section 230 doesn't require us to answer to that politically fraught question, so we won't."

We believe that this Committee is more than capable of reforming Section 230 in ways that fulfill the dual aims of preventing the overexpansion of tech companies' power used to extort profit at the cost of harm to children while fostering a healthy online environment for communications to happen without limited free speech. To do so, we can start by holding tech companies liable for their own representations, recommendations of certain contents, and development of other dangerous product designs.

EISENBERG & BAUM, LLP 24 UNION SQUARE EAST - PENTHOUSE NEW YORK NY 10003 PH 212 353 8700 FAX 917 591 2875 EandBLaw.com

¹ Michael Daly Hawkins & Matthew J. Stanford, *Uproot or Upgrade? Revisiting Section 230 Immunity in the Digital Age*, University if Chicago Law Review Online, https://lawreviewblog.uchicago.edu/2020/06/23/section-230-hawkins-stanford/.

EISENBERG @ BAUM. LLP

For example, Kristin Bride's lawsuit alleged that the anonymous app YOLO overtly stated to users that it will unmask cyberbullies, but when requested by Kristin Bride, it failed to comply with its own representations or even respond to her pleas, four times. Reforming Section 230 so that tech platforms are held accountable based on their own representations, policies, and statements regarding their products would be a starting point that empowers consumers without restricted free speech. Also, recommendation of contents or connection between certain users (i.e., stranger adults and minor children) are algorithms and features that are designed and developed by the tech companies. Holding companies accountable for their direct involvement in developing algorithms designed to perform these specific functions have little to do with third-party content. Lastly, holding companies accountable for dangerously designed products (i.e., anonymous messaging for teens) should be possible under a reformed Section 230. The Committee can develop measures that allow appropriate discovery in early stages of litigation, and through opinions of experts and researchers to establish whether certain designs are dangerous enough to impose liability. This relates back to the proposal articulated in Section 2 that tech companies should bear the burden of proof to provide evidence of effective safety protocols that correspond to the objective dangers and risks of tis product.

Section 230 Should Include Language Allowing Litigants to Calculate Damages 4. Through Data Revenue.

The modernized Section 230 should recognize that we live in a data economy, and that when users are on tech platforms, each minute of usership equates to dollars for Companies. Hence, litigants should be allowed to ask for damages calculations based on the value of their personal data, or conversely, the data revenue that companies profit from users' data.

Carson's family supports the Kids Online Safety Act bill and urges that Section 230 reform is harmonized with its protections.

We thank the Committee's strenuous efforts to make laws that will protect our younger generation and eagerly await your actions.

Kristin Bride

Juyoun Han, on behalf of Carson Bride & Family **Eisenberg & Baum, LLP** 24 Union Square East, Penthouse New York, New York 10003-3201 jhan@eandblaw.com



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

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

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

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

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

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

¹ 47 U.S.C. § 230(e)(5).

333 John Carlyle Street Suite 125 | Alexandria, VA 22314 1-800-THE-LOST® (1-800-843-5678) | MissingKids.org

f y 🖸 🖸 @MissingKids

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



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

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

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

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

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

333 John Carlyle Street Suite 125 | Alexandria, VA 22314 1-800-THE-LOST® (1-800-843-5678) | MissingKids.org

f y 🙆 🗅 @MissingKids

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

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

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

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

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

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

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

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

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

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

2

¹ https://lesp.ncmec.org/LESP/login.

² Some international, federal, and state/local law enforcement agencies use the Case Management Tool, NCMEC's data management interface, to download CyberTipline reports made available to them. ³ Some ICACs use IDS, another data management tool, to download CyberTipline reports made available to them.

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

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

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

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

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

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

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

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

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

4



Question from Senator Whitehouse

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

As Fairplay outlined in the amicus brief it filed with the Supreme Court in *Gonzalez v. Google*, attached, courts have incorrectly extended immunity under Section 230 of the Communications Decency Act to algorithmic recommendation systems and deliberate design choices. Fairplay supports efforts to reform Section 230 to clarify that platform design choices to maximize engagement, including the promotion of content through algorithmic recommendation systems, is not protected publishing activity under the law.

When tech companies design online platforms and build and deploy algorithms, their goal is to maximize user engagement, which in turn maximizes profits. They are not designed to improve young users' wellbeing, nor to serve them high quality content. Ultimately, companies use algorithms and deceptive design techniques to keep kids and teens online for as long as possible, and they use them alongside sophisticated design techniques, including social manipulation and variable reward design features, that target kids' and teens' developmental vulnerabilities.¹ As the Surgeon General has observed, "[b]usiness models are often built around maximizing user engagement as opposed to safeguarding users' health and ensuring that users engage with one another in safe and healthy ways... This translates to technology companies focusing on maximizing time spent, not time well spent."²

Increased time on social media is linked to serious physical and mental health harms for minors. It displaces sleep and physical activity, and the pressure to spend more time on digital media platforms and maximize interactions with other users also puts children at risk of predation. It is also linked with worse psychological wellbeing: Heavy users of digital media are more likely to be unhappy, to be depressed, or to have attempted suicide.³ Two nationally representative surveys of U.S. adolescents in grades 8 through 12 found "a clear pattern linking screen activities with higher levels of depressive symptoms/suicide-related outcomes and nonscreen activities with lower levels."⁴ A large and growing

Fairplay 89 South Street, Suite 403 Boston, MA 02111 fairplayforkids.org

¹ Written Testimony at 10-15.

² Protecting Youth Mental Health: The U.S. Surgeon General's Advisory at 25 (2021),

https://www.hhs.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf.

³ Jean M. Twenge & W. Keith Campbell, *Media Use Is Linked to Lower Psychological Well-Being: Evidence from Three Datasets*, 90 Psychol. Q., 311 (2019). <u>https://pubmed.ncbi.nlm.nih.gov/30859387/</u>

⁴ Jean M. Twenge et al., Increases in Depressive Symptoms, Suicide-Related Outcomes, and Suicide Rates Among U.S. Adolescents After 2010 and Links to Increased New Media Screen Time, 6 Clinical Psychol. Sci. 3, 9 (2018)

body of research indicates a strong link between time spent on social media—some of the services most relentless in their deployment of engagement-maximizing techniques—and serious mental health challenges.⁵ More frequent and longer social media use is associated with depression,⁶ anxiety,⁷ and suicide risk factors.⁸ Increased time on social media can also lead to heightened exposure to content which increases minors' susceptibility to poor body image and, consequently, disordered eating.⁹ Personal stories from sufferers of disordered eating have highlighted the link to social media,¹⁰ as has Meta's own internal research; the documents Frances Haugen shared with the *Wall Street Journal* in 2021 revealed that Facebook has been aware at least since 2019 that "[w]e make body image issues worse for one in three teen girls."¹¹

In addition, maximizing time and activities online also fosters "problematic internet use"—psychologists' term for excessive internet activity that exhibits addiction, impulsivity, or compulsion.¹² A 2016 nationwide survey of minors ages 12 to 18 found that 61% of teens thought they spent too much time

Nature Comm., 1649, (2022), 10.1038/s41467-022-29296-3

⁷ Royal Society for Public Health, #StatusOfMind: Social Media and Young People's Mental Health and Wellbeing 8 (May 2017), <u>https://www.rsph.org.uk/static/uploaded/d125b27c-0b62-41c5-a2c0155a8887cd01.pdf</u>

https://doi.org/10.1177/2167702617723376. See also Jane Harness et al., Youth Insight About Social Media Effects on Well/III-Being and Self-Modulating Efforts, 71 J. Adolescent Health, 324-333 (Sept. 1, 2022), 10.1016/j.jadohealth.2022.04.011; Amy Orben et al., Windows of Developmental Sensitivity to Social Media, 13

⁵ See, e.g., K.E. Riehm et al., Associations Between Time Spent Using Social Media and Internalizing and Externalizing Problems Among US Youth, 76 JAMA Psychiatry, 1266 (2019),

https://doi.org/10.1001/jamapsychiatry.2019.2325; N. McCrae et al., Social Media and Depressive Symptoms in Childhood and Adolescence: A Systematic Review, 2 Adolescent Res. Rev., 315 (2017).

https://doi.org/10.1007/s40894-017-0053-4; H. Allcott et al., *The Welfare Effects of Social Media*, 110 Econ. Rev. Am. 629 (2020), https://www.aeaweb.org/articles?id=10.1257/aer.20190658

⁶ Jean M. Twenge & W. Keith Campbell, Media Use Is Linked to Lower Psychological Well-Being: Evidence from Three Datasets, 90 Psychol. Q. at 312 (2019). https://pubmed.ncbi.nlm.nih.gov/30859387/

⁸ Jean M. Twenge & W. Keith Campbell, Media Use Is Linked to Lower Psychological Well-Being: Evidence from Three Datasets, 90 Psychol. Q. (2019). <u>https://pubmed.ncbi.nlm.nih.gov/30859387/</u>

⁹ A 2019 study of 7th and 8th graders in the International Journal of Eating Disorders "suggest[ed] that [social media], particularly platforms with a strong focus on image posting and viewing, is associated with elevated [disordered eating] cognitions and behaviors in young adolescents." Simon M. Wilksch et al., *The Relationship Between Social Media Use and Disordered Eating in Young Adolescents*, 53 Int. J. Eat. Disord. 96, 104 (2020); see also Pixie G. Turner & Carmen E. Lefevre, Instagram Use Is Linked to Increased Symptoms of Orthorexia Nervosa, 22 Eating Weight Disorders 277, 281 (2017)

¹⁰ See, e.g., Jennifer Neda John, Instagram Triggered My Eating Disorder, Slate (Oct. 14, 2021), https://slate.com/technology/2021/10/instagram-social-media-eating-disorder-trigger.html; Clea Skopeliti, 'I Felt My Body Wasn't Good Enough': Teenage Troubles with Instagram, The Guardian (Sep. 18, 2021), https://www.theguardian.com/society/2021/sep/18/i-felt-my-body-wasnt-good-enough-teenage-troubles-withinstagram.

¹¹ Georgia Wells et al., *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, W.S.J. (Sept. 14, 2021), https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.

¹² Chloe Wilkinson et al., *Screen Time: The Effects on Children's Emotional, Social, and Cognitive Development,* Informed Futures, at 6, (2021), https://informedfutures.org/wp-content/uploads/Screen-time-The-effects-onchildrens-emotional-social-cognitive-development.pdf.

on their mobile devices, and 50% felt "addicted" to them.¹³ In a 2022 Pew Research survey, 35% of teens said they are on YouTube, TikTok, Instagram, Snapchat, or Facebook "almost constantly."¹⁴ And a report released this year by Amnesty International on young people ages 13-24 found "a staggering 74% of respondents report checking their social media accounts more than they would like to.¹⁵ Problematic internet use, in turn, is linked to a host of additional problems.¹⁶

As Fairplay outlined in its attached amicus brief, courts' misinterpretation of Section 230 has prevented tech companies from being held accountable for the harms that result from the deliberate design choices they make. Section 230 should not be altered or repealed such that it no longer provides tech companies protection from liability for the mere presence of user-generated speech. However, the algorithmic recommendation systems and design features that tech companies deploy to push content into users' feeds should not receive blanket protection under Section 230 just because the content that is promoted is user-generated. We believe strongly that state and lower federal courts have misinterpreted the plain text of Section 230 and that the Supreme Court has sufficient evidence to correct these misinterpretations in *Gonzalez*, but we support Congressional action if the Court's decision does not make clear that Section 230 immunity does not extend to platform design choices that maximize engagement.

https://www.amnesty.org/en/latest/news/2023/02/children-young-people-social-media-survey-2/.

149

¹³ Common Sense, *Dealing with Devices: Parents*, 10-11, (2016), <u>https://www.commonsensemedia.org/sites/default/files/research/report/commonsense dealingwithdevices-topline release.pdf.</u>

¹⁴ Emily A. Vogels et al., *Teens, Social Media and Technology 2022,* Pew Research Center (Aug. 10, 2022), https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022.

¹⁵ Amnesty International, "We are totally exposed": Young people share concerns about social media's impact on privacy and mental health in global survey (Feb. 7, 2023)

¹⁶ For example, one study of 564 children between the ages of 7 and 15 found that problematic internet use was positively associated with depressive disorders, Attention Deficit Hyperactivity Disorder, general impairment, and increased sleep disturbances. Restrepo et al., *Problematic Internet Use in Children and Adolescents: Associations with Psychiatric Disorders and Impairment*, 20 BMC Psychiatry 252 (2020), https://doi.org/10.1186/s12888-020-02640-x.

No. 21-1333

IN THE Supreme Court of the United States

REYNALDO GONZALEZ, et al.,

Petitioners,

v.

GOOGLE LLC,

Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit

BRIEF OF FAIRPLAY AS AMICUS CURIAE IN SUPPORT OF PETITIONER REYNOLDO GONZALEZ, ET AL.

ANGELA J. CAMPBELL Counsel of Record PROFESSOR EMERITUS GEORGETOWN LAW 600 New Jersey Ave. NW Washington, D.C. 20001 (202) 662-9541 campbeaj@georgetown.edu

Counsel for Amicus Curiae

December 6, 2022

WILSON-EPES PRINTING CO., INC. - (202) 789-0096 - WASHINGTON, D.C. 20002

TABLE OF CONTENTS

151

TABL	E OF AUTHORITIES	iii
INTE	REST OF AMICUS CURIAE	1
SUMI	MARY OF ARGUMENT	2
ARGU	JMENT	3
I.	AMERICAN YOUTH ARE EXPE- RIENCING MENTAL HEALTH CRISES RESULTING FROM PRODUCTS AND PRACTICES EMPLOYED BY SOCIAL MEDIA COMPANIES	3
	A. Social Media and Youth Mental Health	3
	B. Eating Disorders	6
	C. Social Media Addiction	9
	D. Depression	10
	E. Sleep Deprivation	11
	F. Algorisms Create Mental Health Harms	13
II.	SOCIAL MEDIA COMPANIES DESIGN AND OPERATE THEIR ALGORITHMS TO USE PSYCHOLOGICAL MANIPU- LATION TO MAXI-MIZE ENGAGE- MENT AMONG YOUNG USERS, DIRECTING THEM TO HARMFUL CONTENT THEY DO NOT WANT TO SEE.	14

ii

TABLE OF CONTENTS—Continued

Page

A. The Ninth Circuit's Assumption that Algorithmic Recommendation Systems Are Based on User Preferences Misapprehends How Algorithms Actually Work	14
B. Predominant Algorithmic Design Features	16
1. Low Friction Rewards	16
2. Navigation Manipulation	19
3. Social Manipulation	20
III. ALGORITHMIC RECOMMENDATION SYSTEMS DESIGNED TO MAXIMIZE MINORS' ENGAGEMENT THROUGH PSYCHOLOGICAL MANIPULATION ARE NOT PROTECTED PUBLISHING ACTIVITY	21
A. As Its Text and History Show, Section 230 Was Enacted to <i>Protect</i> Minors From Harmful Exposures to Online Content	21
B. Expansive Interpretation of Section 230(c)(1) Subverts its Statutory Purpose to Protect Children from Online Abuse.	24
C. Algorithms that Use Psychological Manipulation to Maximize Youth Engagements with Online Platforms Are Not Protected Publishing	
Activities	30
CONCLUSION	33

iii

TABLE OF AUTHORITIES

CASES

A.M. v. Omegle.com, No. 3:21-cv-01674, 2022 WL 2713721 (D. Or. July 13, 2022)
Air & Liquid Sys. Corp. v. DeVries, 203 L. Ed. 2d 373, 139 S. Ct. 986 (2019)
Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003)
Doe v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016)24, 25
Doe v. Facebook, Inc., 142 S. Ct. 1087 (2022)
Doe v. MySpace, Inc., 528 F.3d 413 (5th Cir. 2008)
Doe #1 v. MG Freesites, LTD, No. 7:21-cv-00220-LSC, 2022 WL 407147 (N.D. Ala. Feb. 9, 2022)
Does 1-6 v. Reddit, Inc., 51 F.4th 1137 (9th Cir. 2022)
 Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1163 (9th Cir. 2008) 22, 27
Force v. Facebook, Inc., 934 F.3d 53 (2d Cir. 2019)passim
<i>F.T.C. v. Accusearch Inc.,</i> 570 F.3rd 1187 (10th Cir. 2009)

iv

TABLE OF AUTHORITIES—Continued

Gonzalez v. Google LLC, 2 F.4th 871 (9th Cir. 2021)
In re Facebook, Inc, 625 S.W.3d 80 (Tex. 2021)25, 26
In re Social Media Adolescent Addiction / Personal Injury Products Liability Litigation, No. 4:22-md-03047-YGR (N.D. Cal.) 29, 30
Lemmon v. Snap, Inc. 995 F.3d 1085 (9th Cir. 2021)
Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 208 L. Ed. 2d 197, 141 S. Ct. 13 (2020)
Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc., 591 F.3d 250 (4th Cir. 2009)
Rodriquez v. Meta Platforms, et, al, No. 3:22-cv-00401-JD (N.D. Cal.)
Universal Comme'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413 (1st Cir. 2007)
Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997)
STATUTES
47 U.S.C. § 230passim
47 U.S.C. § 230(b)(4) 22, 23

v

TABLE OF AUTHORITIES—Continued

Pag	ge(s)
47 U.S.C. § 230(c)	2, 24
47 U.S.C. § 230(c)(1)pas	ssim
47 U.S.C. § 230(e)(5)	25
RULES	
Fed. R. Civ. P. 12(b)(6)	28
COURT FILINGS	
 Brief for the State of Texas and 24 Other States as Amici Curiae in Support of Petitioner, Doe v. Facebook, Inc., 142 S. Ct. 1087 (Oct. 27, 2022) (No. 21-459) Case Management Order No. 1, In re Social Media Adolescent Addiction/Personal Injury Products Liability Litigation, No. 4:22-md-03047-YGR (N.D. Cal. Nov. 10, 2022) 	26 30
Petition for a Writ of Certiorari, <i>Gonzalez</i> v. <i>Google</i> , No. 21-1333, 2022 WL 1050223 (2021)	30
OTHER AUTHORITIES	
141 Cong. Rec. 3,202 (Feb. 1, 1995)	23
141 Cong. Rec. 15,503 (June 9, 1995)	23

vi

TABLE OF AUTHORITIES—Continued

Among teens, sleep deprivation an epidemic, Stanford News Ctr. (Oct. 8, 2015), https://med.stanford.edu/news/all- news/2015/10/among-teens-sleep-deprivati	10
on-an-epidemic.html Anna Hartford & Dan J. Stein, <i>Attentional</i> <i>Harms and Digital Inequalities</i> , 9 JMIR	12
Mental Health 2 (Feb. 11, 2022), https:// pubmed.ncbi.nlm.nih.gov/35147504/ 1	7, 18
 B. F. Skinner, Two Types of Conditioned Reflex: A Reply to Konorski and Miller, 16 J. Gen. Psychology 272 (1937), https:// doi.org/10.1080/00221309.1937.9917951 	16
Cecilie Schou Andreassen, Torbjørn Torsheim, Geir Scott Brunborg & Ståle Pallesen, Development of a Facebook Addiction Scale, 110 PSYCH. REPS. 501 (2012)	9
Chih-Hung Ko, Ju-Yu Yen, Sue-Huei Chen, Ming-Jen Yang, Huang-Chi Lin & Cheng-Fang Yen, Proposed Diagnostic Criteria and the Screening and Diagnos-	
ing Tool of Internet Addiction in College Students, 50 COMPR. PSYCHIATRY 378 (2009)	9

vii

TABLE OF AUTHORITIES—Continued

 Chung-Ying Lin, Anders Broström, Per Nilsen, Mark D. Griffiths & Amir H. Pakpour, Psychometric Validation of the Persian Bergen Social Media Addiction Scale Using Classic Test Theory and Rasch Models, 6 J. BEHAV. ADDICTIONS 620 (2017) 	9-10
Clea Skopeliti, 'I Felt My Body Wasn't Good Enough': Teenage Troubles with Instagram, The Guardian (Sept. 18, 2021), https:// www.theguardian.com/society/2021/sep/ 18/i-felt-my-body-wasnt-good-enough-tee nage-troubles-with-instagram	7
Chloe Wilkinson et al., Screen Time: The Effects on Children's Emotional, Social, and Cognitive Development (2021), https://informedfutures.org/wp-content/upl oads/Screen-time-The-effects-on-childrens- emotional-social-cognitive-development. pdf	10
Common Sense, <i>Dealing with Devices:</i> <i>Parents</i> (2016), https://www.commonsens emedia.org/sites/default/files/research/re port/commonsense_dealingwithdevices-	
topline_release.pdf	10

viii

TABLE OF AUTHORITIES—Continued

Common Sense, Screens and Sleep: The New Normal: Parents, Teens, Screens, and Sleep in the United States (2019), https://www.commonsensemedia.org/site s/default/files/research/report/2019-new- normal-parents-teens-screens-and-sleep- united-states-rep ort.pdf	12
Danielle Keats Citron & Benjamin Wittes, <i>The Internet Will Not Break: Denying</i> <i>Bad Samaritans § 230 Immunity</i> , 86 FORDHAM L. REV. 401 (2017)	24
Emily A. Vogels et al., <i>Teens, Social Media</i> and <i>Technology 2022</i> , Pew Research Center (Aug. 10, 2022), https://www. pewresearch.org/internet/2022/08/10/tee ns-social-media-and-technology-2022	10
Emily Weinstein & Carrie James, Behind Their Screens: What Teens Are Facing (And Adults Are Missing), MIT Press (2022)	12, 20
Fabrizio Bert et al., <i>Risks and Threats of</i> <i>Social Media Websites: Twitter and the</i> <i>Proana Movement</i> , 19 Cyberpsychology, Behav. Soc. Networking (Apr. 2016), https://pubmed.ncbi.nlm.nih.gov/269918 68/	8
Fairplay, Designing for Disorder: Instagram's Pro-eating Disorder Bubble (Apr. 2022), https://fairplayforkids.org/wp-content/up	0
loads/2022/04/designing_for_disorder.pdf	8

ix

TABLE OF AUTHORITIES—Continued

Farhad Manjoo Jurassic Web The Internet of 1996 is almost unrecognizable compared with what we have today, Slate (Feb. 24, 2009). https://slate.com/technology/2009/ 02/the-unrecognizable-internet-of-1996. html	22
Fatal Injury Reports, National, Regional	
and State, 1981–2020, CTRS. FOR DISEASE CONTROL: WEB-BASED STAT. QUERY & REPORTING SYS., https://wisqars.cdc.gov/	4
fatal-reports (last visited Nov. 17, 2022)	4
GCFGlobal.org, Digital Media Literacy: Why We Can't Stop Scrolling, https://edu.	
gcfglobal.org/en/digital-media-literacy/wh y-we-cant-sto p-scrolling/1/	19
Heavy Social Media Use Linked to Poor Sleep, BBC News (Oct. 23, 2019), https:// www.bbc.com/news/health-50140111	12
Hunt Allcott et al., <i>The Welfare Effects of</i>	12
Social Media, 110 Econ. Rev. Am. 629 (2020), https://www.aeaweb.org/articles?id =10.1257/aer.20190658	6
Hunt Allcott, Matthew Gentzkow & Lena	0
Song, Digital Addiction (Nat'l Bureau of	
Econ. Rsch., Working Paper No. 28936, 2022)	9

х

TABLE OF AUTHORITIES—Continued

J.C. Yau & S. M. Reich, "It's Just a Lot of Work": Adolescents' Self-Presentation Norms and Practices on Facebook and Instagram, 29 J. Res. on Adolescence 196 (2019).	20
J. E. Staddon & D. T. Cerutti, Operant Conditioning, 54 Annual Review of Psy- chology 115 (2003), https://doi.org/10.11 46/annurev. psych.54.101601.145124	16
Jane Harness et al., Youth Insight About Social Media Effects on Well/Ill-Being and Self-Modulating Efforts, 71 J. Ado- lescent Health 324 (Sept. 1, 2022)	6
Jean M. Twenge, A. Bell Cooper, Thomas E. Joiner, Mary E. Duffy & Sarah G. Binau, Age, Period, and Cohort Trends in Mood Disorder Indicators and Suicide-Related Outcomes in a Nationally Representative Dataset, 2005–2017, 128 J. ABNORMAL PSYCH. 185 (2019)	5
Jean M. Twenge, Jonathan Haidt, Jimmy Lozano & Kevin M. Cummins, Specifica- tion Curve Analysis Shows that Social Media Use Is Linked to Poor Mental Health, Especially Among Girls, 224 ACTA PSYCHO- LOGICA, Apr. 2022, Art. No. 103512	5
Jean M. Twenge & W. Keith Campbell, Media Use Is Linked to Lower Psychologi- cal Well-Being: Evidence from Three Datasets, 90 Psychol. Q. 311 (2019)	5,7
	· · ·

TABLE OF AUTHORITIES—Continued

Jean M. Twenge et al., Increases in Depressive Symptoms, Suicide-Related Outcomes, and Suicide Rates Among U.S. Adolescents After 2010 and Links to Increased New Media Screen Time, 6 Clinical Psychol. Sci. 3 (2018)	6
Jeff Chester et al., <i>Big Food, Big Tech, and</i> <i>the Global Childhood Obesity Pandemic</i> (2021), https://www.democraticmedia.org/ sites/default/files/field/public-files/2021/fu ll_report.pdf	12
Jennifer Neda John, <i>Instagram Triggered</i> <i>My Eating Disorder</i> , Slate (Oct. 14, 2021), https://slate.com/technology/2021/10/inst agram-social-media-eating-disorder-trig ger.html	7
Jim Waterson & Alex Hern, Instagram 'Pushes Weight-Loss Messages to Teenagers', The Guardian (Jul 19, 2021, 7:01 AM), https://www.theguardian.com/society/20 21/jul/20/instagram-pushes-weight-loss- messages-to-teenagers	8
K.E. Riehm et al., Associations Between Time Spent Using Social Media and Internalizing and Externalizing Problems Among US Youth, 76 JAMA Psychiatry 1266 (2019), https://doi.org/10.1001/jama	
psychiatry.2019.2325	5

xii

TABLE OF AUTHORITIES—Continued

Konstantinos Ioannidis et al., <i>Cognitive</i> <i>Deficits in Problematic Internet Use: Meta-</i> <i>Analysis of 40 Studies</i> , 215 British Journal of Psychiatry 639, 645 (2019), https:// pubmed.ncbi.nlm.nih.gov/30784392/	11
Laura MacPherson, A Deep Dive into Variable Designs and How to Use Them, DesignLi (Nov. 8, 2018), https://designli. co/blog/a-deep-dive-on-variable-rewards- and-how-to-use-them/	16
Lori Janjigian, What I Learned After Taking Over My 13-Year-Old Sister's Snapchat for Two Weeks, Business Insider (Aug. 4, 2016, 11:53 AM), https://www.business insider.com/how-teens-are-using-snapch at-in-2016	21
Lucy Foulkes and Sarah-Jayne Blakemore, Is There Heightened Sensitive to Social Reward in Adolescence? 40 Current Opinion Neurobiology 81 (2016)	20
Meta, Growth, Friending + PYMK, and down-stream integrity problems, https:// s3.documentcloud.org/documents/233228 45/friending-and-pymk-downstream-inte grity-prob lems.pdf (last visited Dec. 3, 2022)	27
Meta, Integrity Glossary ("PYMK") https:// www.documentcloud.org/documents/233 23294-glossary-of-integrity-terms (last visited Dec. 3, 2022)	27

xiii

TABLE OF AUTHORITIES—Continued

Meta, The Power of Identities: Why Teens and Young Adults Choose Instagram, https://www.documentcloud.org/docume nts/23322855-copy-of-copy-of-why-teens- and-young-adults-choose-insta_sanitized (last visited Dec. 3, 2022)	19
 Michael Kaess et al., Pathological Internet use among European adolescents: psycho- pathology and self-destructive behaviors, 23 Eur. Child & Adolescent Psychiatry 1093 (2014), https://www.ncbi.nlm.nih.gov/ pmc/articles/PMC4229646/ 	11
Michelle A. Miller et al., Sleep Duration and Incidence of Obesity in Infants, Children, and Adolescents: A Systematic Review and Meta-Analysis of Prospective Studies, 41 Sleep 1 (2018), https://pub med.ncbi.nlm.nih.gov/2 9401314/	13
Mike Allen, Sean Parker unloads on Face- book: "God only knows what it's doing to our children's brains", Axios (Nov. 9, 2017), https://www.axios.com/2017/12/15/ sean-parker-unloads-on-facebook-god-only- knows-what-its-doing-to-our-childrens-b rains-15 13306792	18
Mike Brooks, <i>The "Vegas Effect" of Our</i> <i>Screens</i> , Psychol. Today (Jan. 4, 2019), https://www.psychologytoday.com/us/blo g/tech-happy-life/201901/the-vegas-effect- our-screens	17

xiv

TABLE OF AUTHORITIES—Continued

N. McCrae et al., Social Media and Depressive Symptoms in Childhood and Adolescence: A Systematic Review, 2	
Adolescent Res. Rev. 315 (2017), https:// doi.org/10.1007/s40894-017-0053-4	5
Nicholas D. Santer et al., <i>Early Adolescents'</i> <i>Perspectives on Digital Privacy</i> , Algorith- mic Rights and Protections for Children (2021)	20
Nir Eyal, The Hook Model: How to Manufacture Desire in 4 Steps, Nir and Far, https:// www.nirandfar.com/how-to- manufacture-desire/ (last visited Dec. 2, 2022).	17
Pixie G. Turner & Carmen E. Lefevre, Instagram Use Is Linked to Increased Symptoms of Orthorexia Nervosa, 22 Eating Weight Disorders 277 (2017)	7
1 Restatement (Third) of Torts: Liability for Physical and Emotional Harm (2005)	33
Restrepo et al., Problematic Internet Use in Children and Adolescents: Associations with Psychiatric Disorders and Impair- ment, 20 BMC Psychiatry 252 (2020), https://doi.org/10.1186/s12888-020-0264 0-x	1 19

xv

TABLE OF AUTHORITIES—Continued

Rosemary Sedgwick, Sophie Epstein, Rina Dutta & Dennis Ougrin, Social Media, Internet Use and Suicide Attempts in Adolescents, 32 CURRENT OP. PSYCHIATRY	
534 (2019)	5
Royal Society for Public Health, #StatusOfMind: Social Media and Young People's Mental Health and Wellbeing (May 2017)	6
	-
S. Rep. No. 104-230 (1996)	23
Simon M. Wilksch et al., The Relationship Between Social Media Use and Disor- dered Eating in Young Adolescents, 53 Int. J. Eat. Disord. 96 (2020)	7
U.S. SURGEON GEN., ADVISORY: PROTECTING YOUTH MENTAL HEALTH (2021)	4
The Wall Street Journal, Teen Girls Body Image and Social Comparison on Insta- gram – An Exploratory Study in the U.S., Facebook Paper, March 2020 (Sept. 29, 2021), https://digitalwellbeing.org/wp-co ntent/uploads/2021/10/Facebook-Files-Te en-Girls-Body-Image-and-Social-Compar ison-on-Instagram.pdf	7
The Wall Street Journal, How TikTok Serves Up Sex and Drug Videos to Minors	
(September 8, 2021)	9

xvi

TABLE OF AUTHORITIES—Continued

The Wall Street Journal, 'The Corpse Bride Diet': How TikTok Inundates Teens with Eating-Disorder Videos (December 17,	
2021)	9
Yanhui Wu et al., Short Sleep Duration and	
Obesity Among Children: A Systematic	
Review and Meta-Analysis of Prospective	
Studies, 11 Obesity Rsch. & Clinical	
Prac. 140 (2015), https://pubmed.ncbi.	
nlm.nih.gov/27269366/	13

INTEREST OF AMICUS CURIAE¹

Amicus Fairplay is a fiscally sponsored organization of Third Sector New England, Inc., a 501(c)(3) nonprofit that provides information and services to build the knowledge, power, and effectiveness of individuals, organizations, and groups that engage people in community and public life. Fairplay is committed to helping children thrive in an increasingly commercialized, screen-obsessed culture. Fairplay does not accept donations from technology companies or any corporation and is the only organization dedicated to ending online marketing to children. Fairplay's advocacy is grounded in the overwhelming evidence that childtargeted online marketing—and the excessive screen time it encourages—undermines healthy child development.

Amicus Fairplay is deeply interested in this case because the algorithmic recommendation systems and design features at issue in this appeal harm minors by encouraging excessive social media use and directing them to addictive, psychologically destructive, and dangerous online experiences and content. The lower court's decision to expand publisher immunity under 230(c)(1)47 U.S.C. to encompass online §. recommendation algorithms makes it more difficult to hold social media companies accountable for the harms their products inflict on America's children.

¹ No counsel for a party authored any part of this brief and no counsel or party made a monetary contribution intended to fund the preparation or submission of the brief. Only the amici and their attorneys have paid for the filing and submission of this brief. Pursuant to Rule 37.3(a), all parties have granted blanket consent to the filing of amicus curiae briefs.

2 SUMMARY OF ARGUMENT

Rarely in American jurisprudence has the judicial interpretation of a statute been more contrary to the statute's language and legislative history than in the case of 47 U.S.C. § 230(c)(1) (Section 230). The text simply does not support the expansive, all-encompassing immunity asserted by social media companies. Congress enacted Section 230 with the express purpose of *protecting* children from online exposure to obscene materials by granting immunity to companies who remove salacious content from their platforms. Yet lower courts have upended the salutary purpose of Section 230 by extending publisher immunity to social media companies whose algorithms (i) use psychological manipulation to addict vulnerable youth to their platforms, (ii) construct and keep children in dangerous online environments through the algorithmic feeds created by the companies, and (iii) enable child sexual abuse to flourish through their products.

The issue presented here—whether Section 230 immunizes interactive computer services when they make targeted recommendations of information provided by another content provider-has profound implications for society's ability to protect children from the manifest harms associated with social media use. For youth in particular, maximizing online time can lead to a variety of mental and physical health problems and other risks. The lower court's conclusion that social media's algorithmic recommendations are protected publishing activity erroneously assumed those algorithms merely furnish users with content they desire. In fact, the companies expressly design their algorithms to maximize the profits from their online products by creating environments that keep young users online for as long as possible so they will

see more targeted advertising. These purposes go far beyond traditional editorial functions or responding to user requests.

Amicus first explains below that social media usage has led to mental health crises among youth. Amicus then explains how algorithms actually work and why the court below erred in its understanding of algorithms. Finally, Amicus urges this Court to adopt the compelling analysis of the late Chief Judge Robert A. Katzmann in his partial dissent in *Force v. Facebook*, Inc., 934 F.3d 53, 57 (2d Cir. 2019)—cited approvingly by Justice Thomas in Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 17 (2020) (Thomas, J., statement respecting denial of certiorari) and hold that the term "publisher" under § 230(c)(1)reaches only traditional activities of publication (such as deciding whether to publish, withdraw, or alter content) and does not include activities that promote or recommend content or connect users to each other. The Court should reject the expansive interpretation of Section 230 adopted below because it shields social media companies from liability for the harms their products inflict on young people, which is directly contrary to the language and legislative intent of Section 230.

ARGUMENT

I. AMERICAN YOUTH ARE EXPERIENCING MENTAL HEALTH CRISES RESULTING FROM PRODUCTS AND PRACTICES EM-PLOYED BY SOCIAL MEDIA COMPANIES

A. Social Media and Youth Mental Health

In December 2021, United States Surgeon General Vivek Murthy issued an advisory, *Protecting Youth Mental Health*, warning of a mental health crisis

3

among children and young adults caused in part by their overuse of social media. The Surgeon General reported:

From 2009 to 2019, the proportion of high school students reporting persistent feelings of sadness or hopelessness increased by 40%; the share seriously considering attempting suicide increased by 36%; and the share creating a suicide plan increased by 44%. Between 2011 and 2015, youth psychiatric visits to emergency departments for depression, anxiety, and behavioral challenges increased by 28%. Between 2007 and 2018, suicide rates among youth ages 10-24 in the US increased by 57%.

U.S. SURGEON GEN., ADVISORY: PROTECTING YOUTH MENTAL HEALTH 8 (2021). During the same period, the rates of suicide among 12- to 16-year-olds in the United States increased 146%.²

In explaining the crisis' origins, Dr. Murthy noted a "growing concern about the impact of digital technologies, particularly social media, on the mental health and wellbeing of children and young people" and called for greater accountability from social media companies. *Id.* at 25.

Business models are often built around maximizing user engagement as opposed to safeguarding users' health and ensuring that users engage with one another in safe and healthy ways. **This translates to**

4

² Fatal Injury Reports, National, Regional and State, 1981–2020, CTRS. FOR DISEASE CONTROL: WEB-BASED STAT. QUERY & REPORTING SYS., https://wisqars.cdc.gov/fatal-reports (last visited Nov. 17, 2022).

technology companies focusing on maximizing time spent, not time well spent.

5

Id. (emphasis in original).

The Surgeon General's findings are based on an extensive body of research documenting physical and mental health harms to young people resulting from social media use. Many authorities have found a causal relationship between social media and teen suicide,³ and the relationship between social media and other severe mental health outcomes among teens is widely accepted among behavioral health researchers.⁴ Of particular concern is a large and growing body of research indicating a strong link between time spent on social media and serious mental health challenges.⁵

³ See, e.g., Jean M. Twenge, A. Bell Cooper, Thomas E. Joiner, Mary E. Duffy & Sarah G. Binau, Age, Period, and Cohort Trends in Mood Disorder Indicators and Suicide-Related Outcomes in a Nationally Representative Dataset, 2005–2017, 128 J. ABNORMAL PSYCH. 185, 196–97 (2019); Rosemary Sedgwick, Sophie Epstein, Rina Dutta & Dennis Ougrin, Social Media, Internet Use and Suicide Attempts in Adolescents, 32 CURRENT OP. PSYCHIATRY 534, 535, 537, 540 (2019).

⁴ See, e.g., Jean M. Twenge, Jonathan Haidt, Jimmy Lozano & Kevin M. Cummins, Specification Curve Analysis Shows that Social Media Use Is Linked to Poor Mental Health, Especially Among Girls, 224 ACTA PSYCHOLOGICA, Apr. 2022, at 8–10, Art. No. 103512; Jean M. Twenge & W. Keith Campbell, Media Use Is Linked to Lower Psychological Well-Being: Evidence from Three Datasets, 90 Psychol. Q. 311 (2019) (heavy users of digital media are more likely to be unhappy, to be depressed, or to have attempted suicide).

⁵ See, e.g., K.E. Riehm et al., Associations Between Time Spent Using Social Media and Internalizing and Externalizing Problems Among US Youth, 76 JAMA Psychiatry 1266 (2019), https://doi. org/10.1001/jamapsychiatry.2019.2325; N. McCrae et al., Social Media and Depressive Symptoms in Childhood and Adolescence: A Systematic Review, 2 Adolescent Res. Rev. 315 (2017), https://

Two nationally representative surveys of U.S. adolescents in grades 8 through 12 revealed a clear pattern linking screen activities with higher levels of depressive symptoms and suicide-related outcomes and nonscreen activities than with lower levels.⁶ The researchers reported that suicide-related outcomes became elevated after two hours or more a day of electronic device usage, and that, among teens who used electronic devices five or more hours a day, a staggering 48% exhibited at least one suicide risk factor.⁷ Other research associates longer and more frequent social media use with depression,⁸ anxiety,⁹ and suicide risk factors.¹⁰

B. Eating Disorders

Design features that maximize time spent on social media lead to heightened exposure to negative body image and, consequently, eating disorders. A recent study of content 7th and 8th graders "suggest[ed] that [social media], particularly platforms with a strong

 7 Id.

doi.org/10.1007/s40894-017-0053-4; Hunt Allcott et al., *The Welfare Effects of Social Media*, 110 Am. Econ. Rev. 629 (2020), https://www.aeaweb.org/articles?id=10.1257/aer.20190658.

⁶ Jean M. Twenge et al., Increases in Depressive Symptoms, Suicide-Related Outcomes, and Suicide Rates Among U.S. Adolescents After 2010 and Links to Increased New Media Screen Time, 6 Clinical Psychol. Sci. 3, 9 (2018). See also Jane Harness et al., Youth Insight About Social Media Effects on Well/Ill-Being and Self-Modulating Efforts, 71 J. Adolescent Health 324-333 (Sept. 1, 2022).

⁸ Twenge & Campbell, *supra* note 4, at 312.

⁹ Royal Society for Public Health, #StatusOfMind: Social Media and Young People's Mental Health and Wellbeing 8 (May 2017).

¹⁰ Twenge & Campbell, *supra* note 4.

focus on image posting and viewing, is associated with elevated [disordered eating] cognitions and behaviors in young adolescents."¹¹ In another study, researchers found a positive correlation between higher use of Instagram and orthorexia nervosa diagnoses.¹² Personal stories from sufferers of eating disorders have highlighted the link to social media.¹³

Time spent on social media can harm minors' body image and increase their susceptibility to disordered eating in multiple ways. *First*, visual social media triggers social comparison as minors compare their appearance to others, including influencers. An internal Meta study concluded that 66% of teen girls on Instagram experienced negative social comparison, and 52% of that group attributed that experience to viewing beauty-related images on Instagram.¹⁴ *Second*, the companies' recommendation systems

¹¹ Simon M. Wilksch et al., *The Relationship Between Social Media Use and Disordered Eating in Young Adolescents*, 53 Int. J. Eat. Disord. 96, 104 (2020).

¹² Pixie G. Turner & Carmen E. Lefevre, *Instagram Use Is Linked to Increased Symptoms of Orthorexia Nervosa*, 22 Eating Weight Disorders 277, 281 (2017).

¹³ See, e.g., Jennifer Neda John, Instagram Triggered My Eating Disorder, Slate (Oct. 14, 2021), https://slate.com/technolo gy/2021/10/instagram-social-media-eating-disorder-trigger.html; Clea Skopeliti, 'I Felt My Body Wasn't Good Enough': Teenage Troubles with Instagram, The Guardian (Sept. 18, 2021), https:// www.theguardian.com/society/2021/sep/18/i-felt-my-body-wasntgood-enough-teenage-troubles-with-instagram.

¹⁴ The Wall Street Journal, *Teen Girls Body Image and Social Comparison on Instagram – An Exploratory Study in the U.S.*, Facebook Paper, March 2020 (Sept. 29, 2021), https://digital wellbeing.org/wp-content/uploads/2021/10/Facebook-Files-Teen-Girls-Body-Image-and-Social-Comparison-on-Instagram.pdf.

create "bubbles" or "rabbit holes" that funnel users to increasingly extreme content on a given topic¹⁵— topics chosen by the social media company, not by the user. This has proven true for negative body image and eating disorder content.¹⁶

Research shows social media's algorithms have pushed disordered eating and harmful diet techniques to teenage girls.¹⁷ Adolescent girls who express an interest in innocuous topics like fitness tips, general recipes, and healthy eating are bombarded with content targeted to what the algorithms identify as potential insecurities to more extreme content, such as pro-anorexia posts and videos, users, and user groups focused on encouraging others to engage in self-harm and disordered eating. Because the algorithms designed and operated by these companies learn which groups disproportionately engage with this type of content¹⁸ (in this case, female minors), the algorithms generate feeds and recommend connections to young females who do not express any interest in them in order to serve the *companies*' business purpose of keeping the user online and engaged with the product and advertising. There are multiple examples of third parties

¹⁵ Fairplay, Designing for Disorder: Instagram's Pro-eating Disorder Bubble at 1 (Apr. 2022), https://fairplayforkids.org/wp-content/uploads/2022/04/designing_for_disorder.pdf.

 $^{^{16}}$ Id. at 6-7.

¹⁷ See generally id.; Jim Waterson & Alex Hern, Instagram 'Pushes Weight-Loss Messages to Teenagers', The Guardian (Jul 19, 2021, 7:01 AM), https://www.theguardian.com/society/2021/ jul/20/instagram-pushes-weight-loss-messages-to-teenagers.

¹⁸ See Fabrizio Bert et al., Risks and Threats of Social Media Websites: Twitter and the Proana Movement, 19 Cyberpsychology, Behav. Soc. Networking (Apr. 2016), https://pubmed.ncbi.nlm. nih.gov/26991868/.

registering TikTok accounts to fictitious children (as young as 13 to 15), who are then quickly placed in dangerous online experiences by being fed massive amounts of harmful and disturbing content, including paid advertisements targeted by TikTok in a discriminatory manner.¹⁹

C. Social Media Addiction

Medical professionals observed the addictive potential of social media as early as 2009.²⁰ Subsequent research confirmed an addictive paradigm in many social media users' behavior, particularly adolescents.²¹ The Bergen Social Media Addiction Scale²² is now widely used by researchers and mental health professionals to identify and quantify addictive social media behavior.²³ Maximizing time and activities online also

¹⁹ See, e.g., The Wall Street Journal, How TikTok Serves Up Sex and Drug Videos to Minors (September 8, 2021); The Wall Street Journal, 'The Corpse Bride Diet': How TikTok Inundates Teens with Eating-Disorder Videos (December 17, 2021).

²⁰ See, e.g., Chih-Hung Ko, Ju-Yu Yen, Sue-Huei Chen, Ming-Jen Yang, Huang-Chi Lin & Cheng-Fang Yen, Proposed Diagnostic Criteria and the Screening and Diagnosing Tool of Internet Addiction in College Students, 50 COMPREHENSIVE PSYCHIATRY 378 (2009).

²¹ Hunt Allcott, Matthew Gentzkow & Lena Song, *Digital* Addiction 29 (Nat'l Bureau of Econ. Rsch., Working Paper No. 28936, 2022) (finding that "self-control problems magnified by habit formation might be responsible for 31 percent of social media use").

²² Cecilie Schou Andreassen, Torbjørn Torsheim, Geir Scott Brunborg & Ståle Pallesen, *Development of a Facebook Addiction Scale*, 110 PSYCH. REPS. 501 (Apr. 2012), https://pubmed.ncbi. nlm.nih.gov/22662404/.

²³ See, e.g., Chung-Ying Lin, Anders Broström, Per Nilsen, Mark D. Griffiths & Amir H. Pakpour, Psychometric Validation of the Persian Bergen Social Media Addiction Scale Using Classic

fosters "problematic internet use"—psychologists' term for excessive internet activity that exhibits addiction, impulsivity, or compulsion.²⁴

A 2016 nationwide survey found 61% of teens thought they spent too much time on their mobile devices, and 50% felt "addicted" to them.²⁵ In a 2022 Pew Research survey, 35% of teens said they are on YouTube, TikTok, Instagram, Snapchat, or Facebook "almost constantly."²⁶ Over half of teens who describe being online "almost constantly" acknowledged they use social media products too much.²⁷

D. Depression

Problematic internet use is linked to a host of additional problems. For example, in one study of 7 to 15-year-olds, researchers found problematic internet use was positively associated with depressive disorders, Attention Deficit Hyperactivity Disorder, general

Test Theory and Rasch Models, 6 J. BEHAV. ADDICTIONS 620 (Dec. 2017), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6034942/.

²⁴ Chloe Wilkinson et al., *Screen Time: The Effects on Children's Emotional, Social, and Cognitive Development* at 6 (2021), https://informedfutures.org/wp-content/uploads/Screen-time-The-effects-on-childrens-emotional-social-cognitive-development. pdf.

²⁵ Common Sense, *Dealing with Devices: Parents* 10-11 (2016), https://www.commonsensemedia.org/sites/default/files/research/report/commonsense_dealingwithdevices-topline_release.pdf.

²⁶ Emily A. Vogels et al., *Teens, Social Media and Technology* 2022, Pew Research Center (Aug. 10, 2022), https://www.pewrese arch.org/internet/2022/08/10/teens-social-media-and-technology-2022.

 $^{^{27}}$ Id.

11

impairment, and increased sleep disturbances.²⁸ A meta-analysis of peer-reviewed studies involving cognitive findings associated with problematic internet use in both adults and adolescents found "firm evidence that [problematic internet use] . . . is associated with cognitive impairments in motor inhibitory control, working memory, Stroop attentional inhibition and decision-making."29 Another study of over 11,000 European adolescents found that, among teens exhibiting problematic internet use, 33.5% reported moderate to severe depression, 22.2% reported self-injurious behaviors such as cutting, and 42.3% reported suicidal ideation.³⁰ The incidence of attempted suicide was ten times higher for teens exhibiting problematic internet use than for their peers who exhibited healthy internet use.³¹

E. Sleep Deprivation

Maximizing minors' time online at the expense of sleep or movement also harms minors' physical health. Minors who exhibit problematic internet use often

²⁸ Restrepo et al., Problematic Internet Use in Children and Adolescents: Associations with Psychiatric Disorders and Impairment, 20 BMC Psychiatry 252 (2020), https://doi.org/10.1186/s12 888-020-02640-x.

²⁹ Konstantinos Ioannidis et al., *Cognitive Deficits in Problematic Internet Use: Meta-Analysis of 40 Studies*, 215 British Journal of Psychiatry 639, 645 (2019), https://pubmed. ncbi.nlm.nih.gov/30784392/.

³⁰ Michael Kaess et al., *Pathological Internet use among European adolescents: psychopathology and self-destructive behaviors*, 23 Eur. Child & Adolescent Psychiatry 1093, 1096 (2014), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4229646/.

 $^{^{31}}$ Id.

suffer from sleep problems.³² Teenagers who use social media more than five hours per day are about 70% more likely to stay up late on school nights.³³ Onethird of teens say that, at least once per night, they wake up and check their phones for something other than the time, such as to check their notifications or social media.³⁴ Some teens set alarms in the middle of

the night to remind them to check their notifications or complete video game tasks available only for a limited time.³⁵

Sleep deprivation in teenagers is linked to inability to concentrate, poor grades, drowsy-driving incidents, anxiety, depression, suicidal thoughts, and even suicide attempts.³⁶ The increase in time spent online by minors in recent decades has corresponded with increases in youth obesity rates, which in turn increases their risk of serious illnesses like diabetes, high blood pressure, heart disease, and depression.³⁷

³² Restrepo et al., *supra* note 28.

³³ Heavy Social Media Use Linked to Poor Sleep, BBC News (Oct. 23, 2019), https://www.bbc.com/news/health-50140111.

³⁴ Common Sense, Screens and Sleep: The New Normal: Parents, Teens, Screens, and Sleep in the United States at 7 (2019), https://www.commonsensemedia.org/sites/default/files/re search/report/2019-new-normal-parents-teens-screens-and-sleepunited-states-report.pdf.

³⁵ Emily Weinstein & Carrie James, *Behind Their Screens: What Teens Are Facing (And Adults Are Missing)*, MIT Press, at 38 (2022).

³⁶ Among teens, sleep deprivation an epidemic, Stanford News Ctr. (Oct. 8, 2015), https://med.stanford.edu/news/all-news/2015/ 10/among-teens-sleep-deprivation-an-epidemic.html.

³⁷ Jeff Chester et al., *Big Food, Big Tech, and the Global Childhood Obesity Pandemic* at 3 (2021), https://www.democratic media.org/sites/default/files/field/public-files/2021/full_report.pdf.

Sleep deprivation increases the risk of childhood obesity by 20%.³⁸

F. Algorithms Create Mental Health Harms

The youth mental health crisis associated with the rise in social media usage among young Americans is neither an accident nor a coincidence. Rather, as argued below, the harm social media inflicts on young people arises from algorithmic design decisions made by social media companies to maximize minors' engagement with their products. Until social media companies are held accountable for the harms created by their unreasonably dangerous algorithms, this crisis will continue unabated.

³⁸ Yanhui Wu et al., Short Sleep Duration and Obesity Among Children: A Systematic Review and Meta-Analysis of Prospective Studies, 11 Obesity Rsch. & Clinical Prac. 140, 148 (2017), https://pubmed.ncbi.nlm.nih.gov/27269366/; Michelle A. Miller et al., Sleep Duration and Incidence of Obesity in Infants, Children, and Adolescents: A Systematic Review and Meta-Analysis of Prospective Studies, 41 Sleep 1, 15 (2018), https://pubmed.ncbi. nlm.nih.gov/29401314/.

II. SOCIAL MEDIA COMPANIES DESIGN AND OPERATE THEIR ALGORITHMS TO USE PSYCHOLOGICAL MANIPULATION TO MAXIMIZE ENGAGEMENT AMONG YOUNG USERS, DIRECTING THEM TO HARMFUL CONTENT THEY DO NOT WANT TO SEE

A. The Ninth Circuit's Assumption that Algorithmic Recommendation Systems Are Based on User Preferences Misapprehends How Algorithms Actually Work

The Ninth Circuit's holding below—that the algorithmic recommendations online products send to their users are protected publishing activity under Section 230—is premised on the assumption that these recommendations merely furnish users with content they desire:

[A] user's voluntary actions inform Google about that user's preferences for the types of videos and advertisements *the user would like to see....* Google matches what it knows about users based on their historical actions and *sends third-party content to users that Google anticipates they will prefer.* This system is certainly more sophisticated than a traditional search engine, which requires users to type in textual queries, but the core principle is the same: Google's algorithms select the particular content provided to a user based on that user's inputs.

Gonzalez v. Google LLC, 2 F.4th 871, 895 (9th Cir. 2021) (emphasis added). That description betrays a fundamental misunderstanding of how social media algorithms work and impact young users. As Judge

Berzon recognized in her concurrence, "algorithms on social media sites do not offer just one or two suggestions; they operate cumulatively and dominate the user experience. 'The cumulative effect of recommend[ations] . . . envelops the user, immersing her in an entire universe filled with people, ideas, and events she may never have discovered on her own." *Id.* at 917 (quoting Chief Judge Katzmann).

Algorithms that drive social media products are explicitly designed, programmed, and operated for the singular purpose of enhancing revenue by maximizing minor users' engagement with the products. Minors are highly coveted by advertisers and social media is designed to increase the critical commodities of time and activity of minor users.³⁹ For these reasons, user behavior is best understood not as an expression of a user's preference—as the lower court appears to have believed—but as the product of the sophisticated manipulation techniques described throughout this brief. Specifically, content based not on whether a young user will enjoy it, but on whether it will optimize their algorithms feed social media time and activity. To accomplish this pecuniary purpose, companies design and program their products to push content and experiences that trigger a dopamine response in a minor's underdeveloped brain to

³⁹ See, e.g., The Power of Identities: Why Teens and Young Adults Choose Instagram, p. 30 (internal Meta documents identifying and explaining that the "4M teens that start using the internet each year" are the only source for "significant [monthly active user] growth in the US."), https://www.documentcloud. org/documents/23322855-copy-of-copy-of-why-teens-and-youngadults-choose-insta_sanitized (last visited Dec. 3, 2022).

maximize their engagement.⁴⁰ Further, as a matter of basic neurology, content that is dangerous or psychologically discordant triggers a greater dopamine reaction in young users than content that is joyful or benign.⁴¹ Three of the multitude of design features social media companies use to achieve this purpose—low-friction rewards, navigation manipulation, and social manipulation—are discussed below.

B. Predominant Algorithmic Design Features

1. Low-Friction Rewards

Low-friction variable rewards are highly effective at maximizing the time young users spend on social media products. This operant conditioning technique⁴² is based on experiments by psychologist B.F. Skinner.⁴³ Research by Skinner and others revealed that, when test subjects are rewarded unpredictably for a given action, they will engage in the action for longer than if the reward is predictable.⁴⁴ This is because the brain

⁴³ B. F. Skinner, Two Types of Conditioned Reflex: A Reply to Konorski and Miller, 16 J. Gen. Psychology 272-279 (1937), https://doi.org/10.1080/00221309.1937.9917951.

⁴⁴ Laura MacPherson, A Deep Dive into Variable Designs and How to Use Them, DesignLi (Nov. 8, 2018), https://designli.co/ blog/a-deep-dive-on-variable-rewards-and-how-to-use-them/; Mike Brooks, The "Vegas Effect" of Our Screens, Psychol. Today (Jan.

⁴⁰ Wayne Unger, *How the Poor Data Privacy Regime Contributes to Misinformation Spread and Democratic Erosion*, 22 Colum. Sci. & Tech. L. Rev. 308, 323 (2021).

⁴¹ Id.; see also Ronald J. Deibert, The Road to Digital Unfreedom: Three Painful Truths About Social Media, J. Democracy, Jan. 2019, at 25, 29–30.

⁴² J. E. Staddon & D. T. Cerutti, *Operant Conditioning*, 54 Annual Review of Psychology 115–144 (2003), https://doi.org/ 10.1146/annurev.psych.54.101601.145124.

generates more dopamine in response to an uncertain reward than in response to an expected and reliable one.⁴⁵ The tendency of variable rewards to drive compulsive behavior—often referred to as the "Vegas Effect"—is the primary mechanism used in slot machines, keeping players sitting in front of machines for hours.⁴⁶

For years, social media companies have refined and incorporated variable reward designs to drive engagement. As noted psychology expert Nir Eyal has explained, "[v]ariable schedules of reward are one of the most powerful tools that companies use to hook users."⁴⁷ Meta's first President, Sean Parker, described the design as follows:

God only knows what it's doing to our children's brains. The thought process that went into building these applications, Facebook being the first of them, . . . was all about: "How do we consume as much of your time and conscious attention as possible?" And that means that we need to sort of give you a little dopamine hit every once in a while, because someone liked or commented on a

^{4, 2019),} https://www.psychologytoday.com/us/blog/tech-happy-life/201901/the-vegas-effect-our-screens.

⁴⁵ Anna Hartford & Dan J. Stein, *Attentional Harms and Digital Inequalities*, 9 JMIR Mental Health 2, 3 (Feb. 11, 2022), https://pubmed.ncbi.nlm.nih.gov/35147504/ ("At the level of our neural reward system, an uncertain reward generates a more significant dopamine response than those generated by a reliable reward.").

⁴⁶ Brooks, *supra* note 44.

⁴⁷ Nir Eyal, *The Hook Model: How to Manufacture Desire in 4 Steps*, Nir and Far, https://www.nirandfar.com/how-to-manufact ure-desire/ (last visited Dec. 2, 2022).

photo or a post or whatever. And that's going to get you to contribute more content, and that's going to get you . . . more likes and comments. It's a social-validation feedback loop . . . exactly the kind of thing that a hacker like myself would come up with, because you're exploiting a vulnerability in human psychology. The inventors, creators . . . understood this consciously. And we did it anyway.⁴⁸

Today, social media products use machine learning to fine-tune variable rewards, thereby ensuring maximum appeal to each user.⁴⁹ More importantly, social media companies *know* children are more vulnerable to these designs and manipulation techniques, including because of developmental differences. For example, in a document entitled The Power of Identities: Why Teens and Young Adults Choose Instagram, Meta explains that,

The teenage brain is usually about 80% mature. The remaining 20% rests in the frontal cortex

. . . At this time teens are highly dependent on their temporal lobe where emotions, memory, and learning, and the reward system reign supreme . . . Teens' decisions and behavior are mainly driven by emotion, the intrigue of novelty and reward . . .While these all seem positive, they make teens very vulnerable at the elevated levels on which they operate. Especially in the absence of a mature frontal

⁴⁸ Mike Allen, Sean Parker unloads on Facebook: "God only knows what it's doing to our children's brains", Axios (Nov. 9, 2017), https://www.axios.com/2017/12/15/sean-parker-unloads-on-fa cebook-god-only-knows-what-its-doing-to-our-childrens-brains-151 3306792.

⁴⁹ Hartford & Stein, *supra* note 45.

cortex to help impose limits on the indulgence in these. ⁵⁰

A common example of variable rewards is the endless scroll mechanism deployed across social media products. Endless scrolls continuously feed users more content, with no endpoint, as they scroll down a feed or page, and users can never predict what will come next or how interesting it will be. The user is rewarded at unpredictable intervals and levels with content they find funny, entertaining, or otherwise interesting.⁵¹

2. Navigation Manipulation

Online products use various tools to manipulate navigation and prolong user engagement—impeding young users' ability to navigate a website or app to their desired destination. Some design features manipulate navigation to make it harder for a user to leave the service. Others undermine user autonomy by manipulating navigation to encourage users to continue certain activities that are beneficial for the product, such as watching advertisements users did not select and otherwise would not watch. These product designs are implemented to maximize user time and activity at the expense of user safety.

Common examples of navigation manipulation include autoplay and strategically timed advertisements. These techniques make it hard for minors to navigate the online website or service because they either keep the minor on one content stream (increasing time on a

 $^{^{50}}$ See, supra, note 39, at p. 49-74 (section of Meta PowerPoint titled "Teen Fundamentals").

⁵¹ GCFGlobal.org, *Digital Media Literacy: Why We Can't Stop Scrolling*, https://edu.gcfglobal.org/en/digital-media-literacy/why-we-cant-stop-scrolling/1/ (last visited Dec. 2, 2022).

device (autoplay) so as to exclude other content), or they make it difficult, even impossible, for the user to move forward without viewing advertisements. Such navigation manipulation forces users to watch videos or otherwise engage with advertisements either without users' knowledge or irrespective of their preference.

3. Social Manipulation

Manipulative design features that leverage young users' desire for social acceptance are particularly prevalent in social media products. Adolescents have developmental needs for social connectedness and are particularly attuned to social validation.⁵² This can "lead to greater relinquishing of security in certain arenas to gain social validation and belonging-for example, disclosing publicly to participate in online communities and accrue large amounts of likes, comments, and followers."53 Many socially manipulative design features induce anxiety in minors, who come to believe they are not as popular their peers. ⁵⁴ As a result, minors obsess over the popularity of theirs and others' posts. These factors create a feedback loop: Minors crave this social reinforcement, seek it out, and ultimately are ill equipped to protect themselves

⁵² Nicholas D. Santer et al., *Early Adolescents' Perspectives on Digital Privacy*, Algorithmic Rights and Protections for Children (2021) at 6, 30.

⁵³ Id. at 6 (citing J.C. Yau & S. M. Reich, "It's Just a Lot of Work": Adolescents' Self-Presentation Norms and Practices on Facebook and Instagram, 29 J. Res. on Adolescence 196, 196-209 (2019)).

⁵⁴ Weinstein & James, *supra* note 35, at 33 (citing Lucy Foulkes and Sarah-Jayne Blakemore, *Is There Heightened Sensitive to Social Reward in Adolescence?* 40 Current Opinion Neurobiology 81 (2016)).

against the allure of "rewards" these social media designs promise.

One way social media products use social manipulation to increase minor users' engagement is through quantified popularity metrics. These design features gamify popularity by displaying (publicly, privately, or both) the number of friends or connections a user has and the number of interactions their content has received. Such tallies act as quantified proof of popularity and exploit minors' natural tendency to pursue social relevance. The Snapchat "streaks" feature, for example, displays a graphic measurement of young users' level of social interaction on their profiles. Encouraging minors to enlarge their "streaks" by increasing the time spent online generates harmful social pressure and anxiety.⁵⁵

III. ALGORITHMIC RECOMMENDATION SYS-TEMS DESIGNED TO MAXIMIZE MINORS' ENGAGEMENT THROUGH PSYCHOLOG-ICAL MANIPULATION ARE NOT PRO-TECTED PUBLISHING ACTIVITY

A. As Its Text and History Show, Section 230 Was Enacted to *Protect* Minors From Harmful Exposures to Online Content

The Communication Decency Act (CDA) was enacted in 1996 when just seven percent of Americans had access to the Internet, Netscape was the dominant search engine, Google did not exist, and Facebook's

⁵⁵ Lori Janjigian, What I Learned After Taking Over My 13-Year-Old Sister's Snapchat for Two Weeks, Business Insider (Aug. 4, 2016), https://www.businessinsider.com/how-teens-areusing-snapchat-in-2016.

launch was eight years away.⁵⁶ Entitled "Protection for private blocking and screening of offensive material," Section 230 reflected a Congressional finding that "it is the policy of the United States to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material." 47 U.S.C. § 230(b)(4). In

propriate online material." 47 U.S.C. § 230(b)(4). In furtherance of this policy, Section 230(c)—entitled "Protection for 'Good Samaritan' blocking and screening of offensive material"—provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1). This nuanced text simply does not bear the weight that many courts have given to it. It certainly cannot be read to provide overarching immunity for social media products.

Nor does Section 230's history support disregarding the plain text. Quite the contrary. The late Chief Judge Katzmann observed that "[t]he text and legislative history of [§ 230(c)(1)] shout to the rafters Congress's focus on reducing children's access to adult material." *Force*, 934 F.3d at 88 (Katzmann, C.J., dissenting in part); *see also Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1163 (9th Cir. 2008) (en banc) (Section 230 was enacted to protect interactive content providers who *restrict* access to objectionable material). Senator Exon introduced Section 230 to reduce the proliferation of pornography and other obscene material online

⁵⁶ Farhad Manjoo *Jurassic Web The Internet of 1996 is almost unrecognizable compared with what we have today*, Slate (Feb. 24, 2009). https://slate.com/technology/2009/02/the-unrecognizable-internet-of-1996.html.

by subjecting to civil and criminal penalties those who use interactive computer services to make, solicit, or transmit offensive material. 141 Cong. Rec. 3,202 (Feb. 1, 1995). He explained that "[t]he heart and the soul" of the amendment was "protection for families and children." Id. at 15,503 (June 9, 1995). In the House, the Cox-Wyden "Online Family Empowerment" Amendment sought to empower interactive computer service providers to self-regulate, and to provide tools for parents to regulate, children's access to inappropriate material. See S. Rep. No. 104-230, at 194 (1996) (Conf. Rep.); 141 Cong. Rec. 22,045 (Aug. 4, 1995). Congressmen Cox explained that, "[a]s the parent of two, I want to make sure that my children have access to this future and that I do not have to worry about what they might be running into online. I would like to keep that out of my house and off my computer." 141 Cong. Rec. 22,045 (Aug. 4, 1995). Likewise, (then) Congressman Wyden related that "[w]e are all against smut and pornography, and, as the parents of two small computer-literate children, my wife and I have seen our kids find their way into these chat rooms that make their middle-aged parents cringe." Id.

In passing Section 230, "Congress was focused squarely on protecting minors from offensive online material, and that it sought to do so by 'empowering parents to determine the content of communications their children receive through interactive computer services." *Force*, 934 F.3d at 80 (Katzmann, C.J., dissenting in part) (*quoting* legislative history.) Put another way, "Congress enacted Section 230. . . to incentivize [interactive computer service providers] to *protect* children, not immunize them for intentionally or recklessly harming them." *Doe #1 v. MG Freesites, LTD*, No. 7:21-cv-00220-LSC, 2022 WL 407147, at *22 (N.D. Ala. Feb. 9, 2022) (citing 47 U.S.C. § 230(b)(4)) (emphasis in original).

B. Expansive Interpretation of Section 230(c)(1) Subverts its Statutory Purpose to Protect Children from Online Abuse

Numerous federal and state courts have misinterpreted Section 230 by "constru[ing it] broadly in favor of immunity." Force, 934 F.3d at 64; see, e.g., Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc., 591 F.3d 250, 254 (4th Cir. 2009) ("courts have generally accorded Section 230 immunity a broad scope."); Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 419 (1st Cir. 2007) ("Section 230 immunity should be broadly construed."); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003) ("reviewing courts have treated § 230(c) immunity as quite robust."). As two leading scholars have noted, these holdings have "produced an immunity from liability that is far more sweeping than anything the law's words, context, and history support."57 Through this incorrect, broad construction, internet providers "have been protected from liability even though they republished content knowing it might violate the law, encouraged users to post illegal content, [and] changed their design and policies for the purpose of enabling illegal activity." Id.

This overly expansive application of Section 230 also has impeded efforts to combat online exploitation and abuse of vulnerable children. A stark example is *Doe v. Backpage.com, LLC*, 817 F.3d 12 (1st Cir. 2016), which involved a lawsuit by three women who, beginning at age 15, were sex trafficked through advertisements posted on the "Adult Entertainment" section of the Backpage website. These advertisements

⁵⁷ Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401, 408 (2017) (emphasis added).

included photographs of the plaintiffs and coded terminology such as "brly legal" or "high schl" meant to refer to underage girls. Id. at 16-17. Backpage argued that, because the plaintiffs' harms arose from publication of the sex traffickers' content on its platform, their claims were barred by Section 230. Regrettably, the First Circuit agreed, reasoning that the sex trafficking victims sought to hold Backpage liable for "choices about what content can appear on the website and in what form," which are "editorial choices that fall within the purview of traditional publisher functions." Id. at 21. Similarly, in Doe v. *MySpace*, *Inc.*, 528 F.3d 413 (5th Cir. 2008), a minor sexually assaulted by a predator she met through the defendant's product argued that Myspace "fail[ed] to implement basic safety measures to protect minors" from online predators. Id. at 418–20. In holding the child's claims were barred under Section 230(c)(1), the Fifth Circuit characterized her failure to protect claims as "merely another way of claiming that [the website operator] was liable for publishing . . . online third party-generated content." Id. at 420.58

Last year, in *In re Facebook, Inc*, 625 S.W.3d 80 (Tex. 2021), *cert. denied sub nom. Doe v. Facebook, Inc.*, 142 S. Ct. 1087 (2022), the Texas Supreme Court invoked Section 230(c)(1) to bar claims of three minor sex trafficking victims who became "entangled" with

⁵⁸ Public outcry over the *Backpage* and *MySpace* decisions led to the passage of the Stop Enabling Sex Traffickers Act and the Allow States and Victims to Fight Online Sex Trafficking Act of 2018, which eliminated Section 230 as a defense for websites that knowingly facilitate sex trafficking. 47 U.S.C. § 230(e)(5). The Ninth Circuit, however, recently held that, to invoke that exception to Section 230 immunity, a plaintiff must plausibly allege that the website's own conduct violated section 1591. *Does* 1-6 v. *Reddit, Inc.*, 51 F.4th 1137, 1141 (9th Circ 2022).

their abusers through Facebook. Id. at 84–85. In each case, the plaintiffs alleged they were contacted on Facebook or Instagram by adult males, groomed to send naked photographs that were sold over the internet, and ultimately lured into sex trafficking. Id. at 84. The Texas Supreme Court permitted the plaintiffs' statutory human-trafficking claims to proceed but, following Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997) and "abundant judicial precedent," affirmed dismissal of their common law negligence and products liability claims under Section 230(c)(1). Id. at 83, 85–86. Plaintiffs' petition for certiorari was joined by a bipartisan assembly of 24 State Attorney Generals⁵⁹ but denied by this Court on procedural grounds. While agreeing review was premature, Justice Thomas spoke of the human consequences allowed by the broad construction of Section 230:

[T]he Texas Supreme Court afforded publisher immunity even though Facebook allegedly "knows its system facilitates human traffickers in identifying and cultivating victims," but has nonetheless "failed to take any reasonable steps to mitigate the use of Facebook by human traffickers" because doing so would cost the company users—and the advertising revenue those users generate."

Id. at 1088 (Thomas, J., statement respecting denial of certiorari) (citations omitted).

Expansive interpretation of the term "publisher" in Section 230(c)(1) has distorted the statute's "Good Samaritan" purpose by immunizing companies for

⁵⁹ Brief for the State of Texas and 24 Other States as Amici Curiae in Support of Petitioner, *Doe v. Facebook, Inc.*, 142 S. Ct. 1087 (Oct. 27, 2022) (No. 21-459).

their *own* conduct in designing social media algorithms, products, and environments that affirmatively harm children. For example, Meta's algorithmic "friend recommendation" features "People You May Know" and "Suggestions for You" contribute to up to 75% of all inappropriate adult-minor contact on Facebook and Instagram.⁶⁰

As Justice Thomas observed, "[e]xtending § 230 immunity beyond the natural reading of the text can have serious consequences" such as "giving companies immunity from civil claims for knowingly hosting illegal child pornography, or for race discrimination." Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 208 L. Ed. 2d 197, 141 S. Ct. 13, 18 (2020) (citations and quotations omitted) (comment of Thomas, J., on denial of certiorari). Although the Ninth Circuit has acknowledged Section 230 "was not meant to create a lawless no-man's-land on the Internet." Roommates. com, 521 F.3d at 1164, Justice Thomas noted that decisions broadly interpreting Section 230 beyond traditional publisher functions have "eviscerated the narrower liability shield Congress included in the statute." Malwarebytes, 141 S. Ct. at 16 (comment of Thomas, J. on denial of certiorari). Chief Judge Katzmann, whom Justice Thomas cited approvingly, similarly observed that expansive interpretations of Section 230(c)(1) "extend a provision that was designed to encourage computer service providers to shield minors from obscene material so that it now immunizes those

⁶⁰ See, e.g. Meta, Growth, Friending + PYMK, and downstream integrity problems, p. 4 (emphasis added), https://s3.documentclo ud.org/documents/23322845/friending-and-pymk-downstream-in tegrity-problems.pdf; (last visited Dec. 3, 2022) see also Meta, Integrity Glossary, p. 39 ("PYMK") https://www.documentcloud. org/documents/23323294-glossary-of-integrity-terms (last visited Dec. 3, 2022).

same providers" for exposing minors to malign content. *Force*, 934 F.3d at 77 (Katzmann, C.J., dissenting in part). It is difficult to identify another example where courts' interpretations have deviated so far from a statute's language and purpose.

Social media companies have repeatedly argued for essentially absolute immunity and, in so doing, have relied on the decision below. For example, *Rodriguez* v. Meta, Platforms, et, al, Case No. 3:22-cv-00401 (N.D. Cal.) arose from the 2021 suicide death of an 11-yearold girl. The complaint alleges that, when Selena Rodriguez was nine years old, she was given a computer tablet and shortly thereafter began using multiple social media products without her mother's knowledge or consent. Selena quickly became addicted to these products and spent increasing amounts of time on them. In addition, the social media companies programmed their algorithms in a manner that directed, connected, and exposed her to predatory and abusive users and overwhelming amounts of harmful content and social comparison features. On July 21, Selena accessed her mother's supply of 2021.Wellbutrin, placed her phone on a table in her bedroom and turned on the video camera for posting to social media. Holding two Wellbutrin pills between her fingers, she looked straight in the camera, tilted her head back, and placed the pills in her mouth. Selena's mother brought suit for wrongful death based on theories of defective product and failure to warn. In seeking dismissal under Rule 12(b)(6) under Section 230, the defendants (Meta, TikTok, and Snap) relied heavily on the decision below in asserting immunity:

. . . Section 230 . . . bars all of Plaintiff's claims, which are fundamentally based on third-party content. Congress enacted Section 230

to promote free expression on the internet. To accomplish that goal, Section 230 forecloses any claim that seeks to impose liability on interactive computer service providers like Defendants for the alleged effects of thirdparty content—including, as in this case, thirdparty content neither condoned nor permitted by the provider. *See*, *e.g.*, *Gonzalez v. Google LLC*, 2 F.4th 871, 897 (9th Cir. 2021).⁶¹

Those defendants also relied on the decision below in arguing that Rodriguez's addictive design claims "clearly are about third-party content—even if the theory is the harm from viewing *too much* content."⁶² And despite the horrific sexual abuse to which Selena was subjected through Defendants' product, they cited the decision below as the latest example where "courts repeatedly have held that Section 230 protects the content-neutral algorithmic recommendation of even undeniably harmful content."⁶³

Similarly, in *A.M. v. Omegle.com*, No. 3:21-cv-01674, 2022 WL 2713721 (D. Or. July 13, 2022), a chat line user sued a chat room under defective product and failure to warn theories. Plaintiff alleged that, when she was a minor, she was connected by Omegle to a man in his late 30s who forced her to send pornographic images and videos. Incredibly, the defendant cited the decision below in arguing that "all the

⁶¹ Rodriguez v. Meta Platforms, Inc., et. al, 3:22-cv-00401-JD (N.D. Cal.), ECF No. 94 at 11. The case is now part of MDL No. 3047, Case No. 4:22-md-03047-YGR, and the MDL court denied without prejudice all pending dispositive motions in its initial case management order.

 $^{^{62}}$ *Id.* at 18.

⁶³ *Id.* at 17.

elements of CDA 230 immunity [were] satisfied." [Doc. 17 at 4] (initial capitalization and bold printing deleted, citing *Gonzalez*). Fortunately, Judge Mosman rejected that argument and ruled that Section 230 did not provide protection: "Here, Plaintiff alleges that Omegle is defectively designed, and that Plaintiff fails to warn child users of adult predators on the website." A.M., 2022 WL 2713721 at *4. As Judge Mosman noted, "Here, Plaintiff's complaint adequately pleads a product liability lawsuit . . . Omegle could have satisfied its alleged obligation to Plaintiff by designing its product differently—for example, by designing a product so that it did not match minors and adults. Plaintiff is not claiming that Omegle needed to review, edit, or withdraw any third-party content to meet this obligation." Id. at *3 (footnote deleted). Judge Mosman plainly understood the proper scope of Section 230. Unfortunately, many other courts—and the social media industry-do not, and inexplicably insist on virtually unlimited immunity that goes beyond anything in the wording or purpose of Section 230.

C. Algorithms that Use Psychological Manipulation to Maximize Youth Engagements with Online Products Are Not Protected Publishing Activities

The question before the Court is whether the Ninth Circuit correctly held that claims against computer services based on their algorithmic feeds to users treat those services 'as the publisher' of the third-party content such that the services are immunized under Section 230. Petition for a Writ of Certiorari, *Gonzalez* v. *Google*, No. 21-1333, 2022 WL 1050223 (U.S. April 4, 2021). Importantly, a majority of the panel (Judges Berzon and Gould) *agreed* with Chief Judge Katzmann that, while algorithms target users with third party

content, "it strains the English language to say that in targeting and recommending these writings to users and thereby forging connections, developing new social networks [companies are] acting as 'the *publisher* of . . . information provided by another information content provider." Force, 934 F.3d at 63-64 (Katzmann, C.J., dissenting in part) (quoting 47 U.S.C. § 230(c)(1) (emphasis in original)). Accord Gonzalez v. Google LLC, 2 F.4th 871, 913 (9th Cir. 2021) ("For the reasons compellingly given by Judge Katzmann in his partial dissent in Force v. Facebook . . . if not bound by Circuit precedent I would hold that the term "publisher" under § 230 reaches only traditional activities of publication and distribution—such as deciding whether to publish, withdraw, or alter content-and does not include activities that promote or recommend content or connect content users to each other") (Berzon, J, concurring); id. at 918 (Gould, J., dissenting in part) (adopting and attaching Chief Judge Katzmann's dissent). As Judge Berzon observed, "publication has never included selecting the news, opinion pieces, or classified ads to send to each individual reader based on guesses as to their preferences and interests or suggesting that one reader might like to exchange messages with other readers." Id. at 914. As she further noted, "The actions of the social network algorithms—assessing a user's prior posts, friends, or viewing habits to recommend new content and connections-are more analogous to the actions of a direct marketer, matchmaker, or recruiter than to those of a publisher." Id.

As it relates to minors, the algorithms and addictive environments to which social media companies expose children through their social media products are even more attenuated to traditional publishing than the recommendation features derided by Judges Katzmann, Berzon and Gould. Rather than direct users to content 32 Igorithms ar

they "prefer," these algorithms are expressly designed to create an environment that maximizes minors' engagement through psychosocial manipulation that encourages addictive behavior. Algorithms expressly designed to monetize the dopamine responsiveness of adolescent brain function to keep children online bear no relationship to the publishing activity envisioned in Section 230(c)(1). Likewise, algorithms designed to capitalize on adolescents' social anxiety through the use of social comparisons are wholly unrelated to traditional activities of publication such as deciding whether to publish, withdraw, or alter content.

Section 230 does not provide immunity where the harm results from a defendant's "conduct rather than [from] the content of the information." F.T.C. v. Accusearch Inc., 570 F.3rd 1187, 1204 (10th Cir. 2009) (Tymkovich, J, concurring)), quoted in Malwarebytes, Inc., 141 S. Ct. at 18 (statement of Thomas, J., respecting denial of certiorari). Design defect claims alleging that algorithms use psychological manipulation to encourage addictive behavior and knowingly connect vulnerable children to adult predators and malign content do not seek to hold the companies liable "as the publisher or speaker" of third-party content under § 230(c)(1), but "rest[] instead on alleged product design flaws." Malwarebytes, 141 S. Ct. at 18 (Thomas, J.). Accord, e.g., Lemmon v. Snap, Inc. 995 F.3d 1085, 1087 (9th Cir. 2021) (Section 230 does not bar claim for negligent design claim for hazardous feature in social media product). When social media companies design and operate algorithms in ways they know may cause harm to minors, they should be held accountable—just like every other individual or company—for the foreseeable consequences of their deliberate choices. See generally Air & Liquid Sys. Corp. v. DeVries, 139 S. Ct. 986, 993 (U.S. 2019)

(quoting 1 Restatement (Third) of Torts: Liability for Physical and Emotional Harm § 7, p. 77 (2005) ("Tort law imposes 'a duty to exercise reasonable care' on those whose conduct presents a risk of harm to others")).

CONCLUSION

This Court should adopt the persuasive and correct approach to Section 230 urged by the late Chief Judge Katzmann, and by Judges Berzon and Gould below.

Respectfully submitted,

ANGELA J. CAMPBELL Counsel of Record PROFESSOR EMERITUS GEORGETOWN LAW 600 New Jersey Ave. NW Washington, D.C. 20001 (202) 662-9541 campbeaj@georgetown.edu

Counsel for Amicus Curiae

December 6, 2022



Questions from Senator Tillis for Josh Golin, Executive Director of Fair Play

1. What are the largest impacts of high screen time for children? How can this be mitigated?

Excessive screen media use and social media use is linked to a number of risks for children and adolescents, including obesity,¹ lower psychological wellbeing,² decreased happiness,³ decreased quality of sleep,^{4,5} increased risk of depression,⁶ and increases in suicide-related outcomes such as suicidal ideation, plans, and attempts.⁷

Young people who exhibit signs of problematic internet use – psychologists' term for excessive internet activity that exhibits addiction, impulsivity, or compulsion – are particularly at risk. For example, one study of 564 children between the ages of 7 and 15 found that problematic internet use was positively associated with depressive disorders, attention-deficit/hyperactivity disorder (ADHD), general impairment, and increased sleep disturbances.⁸ A meta-analysis of peer-reviewed studies involving cognitive findings associated with problematic internet use in both adults and adolescents found "firm evidence that [problematic internet use]. . . is associated with cognitive impairments in motor inhibitory control, working memory, Stroop attentional inhibition and decision-making."⁹ Another study of over 11,000 European adolescents found that among teens exhibiting problematic internet use, 33.5%

¹ Robinson, T. N., Banda, J. A., Hale L., Lu, A. S., Fleming-Milici, F., Calvert, S. L., Wartella, E. "Screen media exposure and obesity in children and adolescents." *Pediatrics*, 140 (Supplement 2), S97-S101. (2017), doi:<u>10.1542/peds.2016-1758K</u>

² Twenge, J., Campbell, K. "Media Use Is Linked to Lower Psychological Well-Being: Evidence from Three Datasets," *Psychiatric Quarterly* 90, no. 2. 311–31, (1 June 2019), <u>https://doi.org/10.1007/s11126-019-09630-7</u>.
 ³ Twigg, L, Duncan, C., Weich, S. "Is Social Media Use Associated with Children's Well-Being? Results from the UK Household Longitudinal Study," *Journal of Adolescence* 80: 73–83, (1 April 2020), <u>https://doi.org/10.1016/j.adolescence.2020.02.002</u>.

⁴ Carter, Ben et al. "Association Between Portable Screen-Based Media Device Access or Use and Sleep Outcomes: A Systematic Review and Meta-Analysis." *JAMA Pediatrics* 170, no. 12: 1202–8, (1 Dec. 2016), <u>https://doi.org/10.1001/jamapediatrics.2016.2341</u>.

⁵Lemola, Sakari et al. "Adolescents' Electronic Media Use at Night, Sleep Disturbance, and Depressive Symptoms in the Smartphone Age." *Journal of Youth and Adolescence* 44 (1 Feb. 2014), <u>https://doi.org/10.1007/s10964-014-0176-x</u>.

⁶ Ibid.

⁷ Twenge, Jean et al. "Increases in Depressive Symptoms, Suicide-Related Outcomes, and Suicide Rates Among U.S. Adolescents After 2010 and Links to Increased New Media Screen Time." *Clinical Psychological Science* 6, no. 1, 3-17, (1 Jan. 2018), <u>https://doi.org/10.1177/2167702617723376</u>.

⁸ Restrepo et al., Problematic Internet Use in Children and Adolescents: Associations with Psychiatric Disorders and Impairment, 20 BMC Psychiatry 252 (2020), <u>https://doi.org/10.1186/s12888-020-02640-x</u>.
⁹ Konstantinos Joannidis et al., Cognitive Deficits in Problematic Internet Use: Meta-Analysis of 40 Studies, 215

British Journal of Psychiatry 639, 645 (2019), https://pubmed.ncbi.nlm.nih.gov/30784392/.

Fairplay 89 South Street, Suite 403 Boston, MA 02111 fairplayforkids.org

42.3% reported suicidal ideation.¹⁰ The rate of attempted suicides was a staggering ten times higher for teens exhibiting problematic internet use than their peers who exhibited healthy internet use.¹¹

The more time that young people spend online, the greater the chance that they will have negative and unwanted experiences. Fifty-nine percent of US teens have reported being bullied on social media,¹² an experience which has been linked to increased risky behaviors such as smoking and increased risk of suicidal ideation.¹³ The pressure to spend more time on digital media platforms and maximize interactions with other users also puts children at risk from predation. Twenty-five percent of 9- to 17- year-olds report having had an online sexually explicit interaction with someone they believed to be an adult.¹⁴ In 2020, 17% of minors – including 14% of 9- to 12-year-olds – reported having shared a nude photo or video of themselves online. Of these children and teens, 50% reported having shared a nude photo or video with someone they had not met in real life and 41% reported sharing with someone over the age of 18.¹⁵

The best way to mitigate these negative effects is to create a duty of care that requires online operators to prevent and mitigate the most serious harms to young people. The current business model for most digital media revolves around maximizing engagement in order to collect more data and serve more ads. This harms young people in two related ways. First, as noted above, excessive use of digital media is associated with a number of serious harms to young people, in part because time spent online displaces activities with proven developmental benefits. Second, the design choices used by platforms to maximize engagement create new risks. For example, as described below in the answer to question #4, algorithms designed to maximize engagement often recommend harmful content to young people and send them down rabbit holes.

Just as companies currently design their services to prioritize profits and engagement over children's wellbeing, these same services *could* be designed in a way that puts children first. But that won't happen without significant action from Congress, such as passing the Kids Online Safety Act.

¹⁰ Michael Kaess et al., Pathological Internet use among European adolescents: psychopathology and selfdestructive behaviours, 23 Eur. Child & Adolescent Psychiatry 1093, 1096 (2014), <u>https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4229646/.</u>
¹¹ Id

¹² Anderson, Monica. "A Majority of Teens Have Experienced Some Form of Cyberbullying," *Pew Research Center: Internet, Science & Tech* (blog), (27 Sep. 2018), <u>https://www.pewresearch.org/internet/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/.</u>

¹³ Van Geel, M., Vedder, P., Tanilon, J.. "Relationship Between Peer Victimization, Cyberbullying, and Suicide in Children and Adolescents: A Meta-Analysis," *JAMA Pediatrics* 168, no. 5: 435–42, (1 May 2014), <u>https://doi.org/10.1001/jamapediatrics.2013.4143</u>.

 ¹⁴ Thorn. "Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking." (May 2021), <u>https://info.thorn.org/hubfs/Research/Responding%20to%20Online%20Threats_2021-Full-Report.pdf</u>.
 ¹⁵ Thorn. "Understanding sexually explicit images, self-produced by children." (9 Dec. 2020),

https://www.thorn.org/blog/thorn-research-understanding-sexually-explicit-images-self-produced-by-children/.

2. You've raised concern in the past that even EdTech (Educational Technology), in terms of high screen time, can be dangerous for our children. Do you see a path forward where a balance can be struck with EdTech as it does have its benefits in certain situations?

For-profit EdTech vendors are selling schools, families and policymakers on the false premise that EdTech products offer the most effective and budget-friendly ways to learn. In reality, the products are costly to purchase and maintain. The products also ensnare students, whose data and brand loyalty are harvested, and who often become targets of relentless marketing efforts. These efforts include the insidious practice of upselling, through which students and their families are pushed to purchase premium versions, thereby exacerbating inequalities among students.¹⁶ Equally important, these programs reduce the roles played by creative, compassionate teachers in educating the whole child. Learning happens best in the context of human relationships and is lost when the balance is skewed toward online platforms.

The value of face-to-face instruction is well-supported by research.¹⁷ There is no credible research supporting the value of investing heavily in computer technology for schools.¹⁸ Test scores do not rise. Dropout rates do not fall. Graduation rates do not improve. In 2019, fewer than half of virtual and blended schools had "acceptable" state performance ratings, and only 30% of virtual schools associated with for-profit Education Management Organizations (EMO) managed to meet even that low bar.¹⁹ A study of millions of high school students in 36 countries by the Organisation for Economic Co-operation and Development (OECD) found that students who frequently used computers at school "do a lot worse in most learning outcomes, even after accounting for social background and student demographics."²⁰

EdTech is destined to under-deliver because of how the human brain reacts to screen-based media. In short: the brain doesn't like it. Reading text on paper increases comprehension, retention, and sheer satisfaction with reading as an activity.²¹ Writing by hand boosts idea generation as well as retention.²² Children between the ages of 8 and 11 who spend more than two hours per day on screens perform

¹⁶ See, e.g., Campaign for a Commercial-Free Childhood (now Fairplay), "Request for Investigation of Deceptive and Unfair Practices by the Edtech Platform Prodigy." *Campaign for a Commercial-Free Childhood before the Federal Trade Commission*. (19 Feb. 2020). <u>https://fairplayforkids.org/wp-</u>

content/uploads/2021/02/Prodigy_Complaint_Feb21.pdf ¹⁷ See, e.g., Mohammed, Saro. "Tech or No Tech, Effective Learning Is All about Teaching." *Brookings* (blog), September 6, 2018. <u>https://www.brookings.edu/blog/brown-center-chalkboard/2018/09/06/tech-or-no-tech-effective-learning-is-all-about-teaching/</u>.

¹⁸ Molnar, Alex, Gary Miron, Najat Elgeberi, Michael K. Barbour, Luis Huerta, Sheryl Rankin Shafer, and Jennifer King Rice. "Virtual Schools in the U.S. 2019," May 28, 2019. <u>https://nepc.colorado.edu/publication/virtual-schoolsannual-2019</u>; OECD. "Students, Computers and Learning," 2015. <u>https://www.oecdillibrary.org/content/publication/9789264239555-en</u>.

¹⁹ Molnar et al. (2019).

²⁰ OECD (2015).

²¹ Jabr, Ferris. "The Reading Brain in the Digital Age: The Science of Paper versus Screens." *Scientific American*. April 11, 2013. <u>https://www.scientificamerican.com/article/reading-paper-screens/</u>.

²² James, Karin H., and Laura Engelhardt. "The Effects of Handwriting Experience on Functional Brain Development in Pre-Literate Children." *Trends in Neuroscience and Education* 1, no. 1 (December 1, 2012): 32–42. <u>https://doi.org/10.1016/j.tine.2012.08.001</u>.

worse on memory, language, and thinking tests than those who spend less time on screens.²³ The sensorimotor stimuli that screens offer are paltry compared to real life stimuli, and developing brains are more severely impacted by this disparity.²⁴

Nevertheless, EdTech can be an important tool in helping students learn, provided it is used in a responsible, developmentally appropriate and limited way where digital technologies are just one of many tools in the pedagogical tool box. From a policy perspective, the following is needed order to maximize the educational benefits to children of EdTech and limit the harms:

- Congress should expand privacy protections to teens by passing the Children and Teens' Online Privacy Protection Act or similar legislation. The Children's Online Privacy Protection Act (COPPA) is an important tool for protecting student data but it only covers children until their 13th birthday. Teens deserve COPPA's data minimization and use limitation requirements to ensure that the sensitive data collected from them over the course of the school day or for homework is protected.
- 2. The Federal Trade Commission (FTC) should follow through on its important May 2022 Policy Statement on Education Technology and the Children's Online Privacy Protection Act and bring enforcement actions against EdTech companies that collect extraneous student data, violate COPPA's use prohibitions, retain data longer than reasonably necessary to fulfill the purpose for which it collected, or fail to meet COPPA's security requirements.
- The Department of Education and/or Health and Human Services should issue guidance on best practices for EdTech use. Such guidance should include developmentally appropriate limits on screen use in classrooms and for homework.
- 4. Congress should prohibit the use of educational technologies that exert commercial pressure on students. This should include a prohibition on ad-supported services, as advertising on digital platforms that are required for school use exploits a captive audience of students. It should also include a prohibition on using EdTech platforms in schools that sell subscriptions directly to students and their families. Subscriptions create inequities between families who can and cannot afford to pay for extras; in addition, subscription models encourage EdTech companies to design their products to maximize engagement and revenue rather than educational outcomes.

3. What is surveillance advertisement and how is this particularly detrimental to children? How can this be mitigated?

Surveillance advertising – also sometimes called targeted, personalized or behavioral advertising – is the practice of targeting online advertisements to individuals based on their online and offline activities,

 ²³ Walsh, Jeremy J., Joel D. Barnes, Jameason D. Cameron, Gary S. Goldfield, Jean-Philippe Chaput, Katie E. Gunnell, Andrée-Anne Ledoux, Roger L. Zemek, and Mark S. Tremblay. "Associations between 24 Hour Movement Behaviours and Global Cognition in US Children: A Cross-Sectional Observational Study." *The Lancet Child & Adolescent Health* 2, no. 11 (November 1, 2018): 783–91. <u>https://doi.org/10.1016/S2352-4642(18)30278-5</u>.
 ²⁴ Softky, William, and Criscillia Benford. "Sensory Metrics of Neuromechanical Trust." *Neural Computation* 29, no. 9 (June 9, 2017): 2293–2351. <u>https://doi.org/10.1162/neco_a_00988</u>.

behaviors and interests. Surveillance advertising is harmful to children in a number of ways.

First, it leads to massive and invasive data collection. By some estimates, advertisers already possess over 13 million data points about a child by the time they turn 13, despite the fact that the Children's Online Privacy Protection Act (COPPA) requires parental permission before sharing the personal information of children 12 and under with advertisers.²⁵ This data is often shared with opaque networks and actors, making children's sensitive data vulnerable to hacking and misuse.

Second, surveillance advertising is unfair to children. As Fairplay, Global Action Plan, and Reset Australia described in a report about Facebook:

On the one side is a child, poorly equipped to distinguish between advertising and information, especially within digital contexts. On the other, Facebook with its vast troves of data about the child, including but not limited to their browsing history, mood, insecurities, their peers' interests, and more. This power imbalance makes surveillance advertising inherently more manipulative than contextual digital advertising, let alone traditional analogue advertising.²⁶

Third, ads can be used to target and exacerbate young people's vulnerabilities. Leaked documents from Facebook revealed in 2017 that the company told advertisers it could help them target teens at moments when they are feeling specific emotions, such as "silly," "defeated," "overwhelmed," "useless" and "a failure."²⁷ This capability allows marketers to target vulnerable young people with ads for harmful products. Ads for risky "Flat Tummy Teas" and dangerous exercise routines target young women on Instagram. Early digital marketing campaigns for Juul vaping products were deliberately targeted at young audiences.²⁸ Researchers were able to target ads to teenagers on Facebook based on their interests in gambling, alcohol, and dieting.²⁹

Finally, in order to maximize surveillance ad revenue and data collection, platforms are often designed to maximize user engagement. As described in the reply to question #1, this can be harmful to young people by fostering overuse.

https://doi.org/10.1136%2Ftobaccocontrol-2018-054382 ("JUUL was one of the first major retail e-cigarette brands that relied heavily on social media to market and promote its products."); Julia Cen Chen-Sankey et al., Ecigarette Marketing Exposure and Subsequent Experimentation Among Youth and Young Adults, 144 Pediatrics at 8 (Nov. 2019), https://doi.org/10.1542/peds.2019-1119; see also Erik Larson et al., Juul Reaches \$439 Million Settlement Over Marketing to Kids, Bloomberg Law, (Sept. 6, 2022), https://news.bloomberglaw.com/health-lawand-business/juul-reaches-439-million-multi-state-settlement-over-marketing.

²⁵ SuperAwesome Launches Kid-Safe Filter to Prevent Online Ads from Stealing Children's Personal Data, SuperAwesome (Dec. 6, 2018), <u>https://www.superawesome.com/superawesome-launches-kid-safe-filter-to-prevent-online-ads-from-stealing-childrens-personal-data/</u>.

 ²⁶ Yi-ching Ho, E., Farthing, R., *How Facebook still targets surveillance ads to teens*, Reset Australia, Fairplay, and Global Action Plan (Nov. 2021), https://fairplayforkids.org/wp-content/uploads/2021/11/fbsurveillancereport.pdf.
 ²⁷ Sam Machkovech, *Report: Facebook Helped Advertisers Target Teens Who Feel "Worthless"*, ArsTechnica (May 1, 2017), https://arstechnica.com/information-technology/2017/05/facebook-helpedadvertisers-target-teens-who-feel-worthless/.

²⁸ Jidong Huang et al., Vaping versus JUULing: how the extraordinary growth and marketing of JUUL transformed the US retail e-cigarette market, 28 Tobacco Control 146, 150 (Feb. 22, 2019),

²⁹ Farthing, Rys, et al., Profiling Children for Advertising: Facebook's Monetisation of Young People's Personal Data, Reset Australia, (April 2021), <u>https://au.reset.tech/uploads/resettechaustralia_profiling-children-for-advertising-1.pdf</u>.

Prohibiting the use of user data to target ads to minors will mitigate the harms of surveillance advertising on young people. The Children and Teens' Online Privacy Protection Act, which advanced out of the Commerce Committee in 2022 and is expected to be reintroduced soon, would do just that.

4. Beyond surveillance advertisement, are there any other algorithmic-based practices being implemented that are particularly detrimental to children? How can this be mitigated?

In addition to surveillance ads, engagement-maximizing algorithms are detrimental to children. These algorithms fill young people's feeds with the content that is most likely to keep them online, and are one of the primary ways children are exposed to posts, images, or videos that are age-inappropriate, dangerous, or abusive. Platforms such as YouTube, TikTok, and Instagram serve users content based on automated suggestions. Algorithms choose which content to suggest to children and teens based on the vast amount of data they collect on users, such as likes, shares, comments, interests, geolocation, and information about the videos a user watches and for how long. These algorithms are designed to extend engagement by discerning which pieces of content a user is most likely to engage with – not whether the content or overall online experience is beneficial to the user.³⁰

Algorithmic recommendations can be particularly dangerous when they target children and teens' greatest vulnerabilities. Investigations have repeatedly demonstrated the way social media feeds deliver harmful mental health and eating disorder content to accounts registered to minors. A December 2022 report by the Center for Countering Digital Hate (CCDH) found that newly created TikTok accounts registered to teenagers that watched or liked videos about body image, mental health, or eating disorders received videos in their For You feeds related to self-harm, suicide, or eating disorders within minutes.³¹ CCDH also studied the For You feeds of newly created TikTok accounts registered to teenagers that included the phrase "loseweight" in their usernames. Those accounts received videos about self-harm, suicide, or eating disorders in their For You feeds every 66 seconds on average.³²

Other reports have made similar findings: A 2021 *Wall Street Journal* investigation documented how TikTok users were served videos that encouraged eating disorders and discussed suicide.³³ The same year, Senator Richard Blumenthal's office created an account for a fake 13-year-old girl that "liked" content about dieting, and the account was served pro-eating disorder and self-harm content within 24 hours.³⁴ Young users' engagement with this harmful content is valuable to tech companies: Fairplay's

³⁰ A former YouTube engineer observed: "recommendations are designed to optimize watch time, there is no reason that it shows content that is actually good for kids. It might sometimes, but if it does, it is coincidence." Orphanides, K.G. "Children's YouTube is still churning out blood, suicide and cannibalism." *Wired*, (March 23, 2018), <u>https://www.wired.co.uk/article/youtube-for-kids-videos-problems-algorithm-recommend</u> ³¹ Center for Countering Digital Hate, *Deadly by Design: Tik Tok Pushes Harmful Content Promoting Eating Disorders* and Self-harm into users' feeds, (Dec. 15, 2022), <u>https://counterhate.com/research/deadly-by-design/</u>² *i*/*i*

³³ Wall Street Journal Staff, Inside TikTok's Algorithm: A WSJ Video Investigation, Wall Street Journal, (July 21, 2022) https://www.ice.com/actives/acti

^{2021), &}lt;u>https://www.wsj.com/articles/tiktok-algorithm-video-investigation-11626877477</u>. ³⁴ Nihal Krishan, *Senate office impersonates 13-year-old girl on Instagram to flag eating disorder content*, Yahoo News, (Sep. 30 2021), <u>https://www.yahoo.com/entertainment/senate-office-impersonates-13-old-</u> 212700515.html.

2022 report detailed how Meta profits from 90,000 unique pro-eating disorder accounts that reach 20 million people, one-third of whom are minors, some as young as nine.³⁵

Content recommendation algorithms also expose minors to videos of dangerous viral "challenges," which has tragically led to the serious injuries and deaths of many young people. For example, media reports have documented how "the blackout challenge" on TikTok, in which young people hold their breath or choke themselves until they pass out, is responsible for the deaths of several children.³⁶ Many families say that their children learned about the challenge through recommended videos on their For You feeds.³⁷

Policy interventions are needed in order to mitigate the harms of algorithmic recommendation systems on children. For example, the Kids Online Safety Act has a duty of care that requires platforms in their design and operation (including their deployment of algorithms) to prevent and mitigate "mental health disorders or associated behaviors, including the promotion or exacerbation of suicide, eating disorders, and substance use disorders, consistent with evidence-based medical information;" Harmful algorithmic recommendations can also be addressed by prohibiting harmful uses of minors' data.

5. Are you aware of any surveillance advertisements or algorithms that are used to target children, specifically to promote drugs and the sale of narcotics?

This is not my area of expertise so I am not qualified to answer this question. I would encourage anyone interested in this topic to read <u>this newly released report</u> from the Colorado Department of Law. It contains a lengthy section on how illegal drugs are marketed online. I would also encourage you to speak with Eric Feinberg at the Coalition for a Safer Web who tracks the advertising of drugs on social media.

³⁵ Fairplay, Designing for Disorder: Instagram's Pro-eating Disorder Bubble at 1 (Apr. 2022),

https://fairplayforkids.org/wp-content/uploads/2022/04/designing_for_disorder.pdf. ^{3e}Olivia Carville, *TikTok's Viral Challenges Keep Luring Young Kids to Their Deaths*, Bloomberg, (Nov. 30, 2022), https://www.bloomberg.com/news/features/2022-11-30/is-tiktok-responsible-if-kids-die-doing-dangerous-viral-<u>challenges</u>; Anne Marie Lee, *Child deaths blamed on TikTok 'blackout challenge' spark outcry, CBS News*, (Aug. 19, 2021), https://www.cbsnews.com/news/tik-tok-blackout-challenge-child-deaths/.

³⁷ Michael Levenson and April Rubin, Parents Sue TikTok, Saying Children Died After Viewing 'Blackout Challenge', New York Times, (July 6, 2022), <u>https://www.nytimes.com/2022/07/06/technology/tiktok-blackout-challenge-</u> <u>deaths.html</u>.

207

LOG OFF

Senator Sheldon Whitehouse Senate Judiciary Committee Hearing "Protecting Our Children Online" Questions for the Record for Emma Lembke

Submitted March 1, 2023

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

Thank you, Senator Whitehouse, for the opportunity to provide a response to this question. As a youth advocate for safer social media and online platforms for kids, teens, and young adults, I will preface my response in the fact that the policy nuance of the debate over Section 230 reform is outside the scope of my expertise. Thus, I largely defer to my fellow witnesses to provide more substantive responses as to their precise proposed legislative changes to Section 230.

While I recognize the need to update Section 230 — a law written in 1996, before I or anyone else in my generation was born and well before today's internet had been imagined — I believe that Section 230 reform is not the only way we can reduce the harms of social media and Big Tech platforms for kids, teens, and young adults.

It is critical that updates to Section 230 account for the continued evolution of the internet and take into account possible unintended consequences by centering the experiences of young people like myself and others who would be directly affected by Section 230 reform. Simultaneously, I support the advancement of bipartisan policies to protect kids, teens, and young adults online. I believe we must take an "all of the above" approach to rein in Big Tech's societal harms and protect kids, teens, and young adults online.

As I said in my testimony before the Senate Judiciary Committee, "The mental health crisis for young people that we are witnessing will only continue to rise. So, we cannot wait another year, we cannot wait another month, another week, or another day to begin to protect the next generation from the harms that we have witnessed and heard about today."

Senator Sheldon Whitehouse Senate Judiciary Committee Hearing "Protecting Our Children Online" Questions for the Record for John Pizzuro Submitted February 21, 2023

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

There needs to be more accountability within the existing Section 230 Framework. My concern is that if we eliminate immunity, which needs to be changed to make these companies liable for how their platform is used, they will go to end-to-end encryption, thus putting more children in danger.

To receive immunity, social media companies would have to ensure specific remedies are taken place on their platforms, including but not limited to; age verification, identity verification, and AI scanning. We can also require scanning an operating system or browser on the device for CSAM, Grooming, etc.

Judiciary Committee Hearing: Protecting Our Children Online February 14, 2023 Questions for the Record Senator Peter Welch

Questions for Mr. John Pizzuro

Big tech companies are exacerbating the fentanyl crisis—they've turned a blind eye to folks selling drugs on their platforms, giving dealers an easy way to reach buyers online. That's a particular problem for our kids, who can easily buy dangerous drugs through social media platforms.

1. When you served in the New Jersey State Police Department, what challenges did you or your colleagues face in preventing, identifying, and catching these transactions on social media?

Social Media companies themselves. Drug Trafficking Organizations, Cartels, and even independent drug traffickers have transitioned to social media apps and games relying on their chat features instead of using the phone to conduct their business. Law Enforcement is unable to monitor these platforms even with legal processes. End to End Encryption protects companies from the content on their platforms.

If I were a Mexican Cartel, for example, that traffics Fentanyl, I would rely explicitly on social media to conduct my business. I can communicate without fear of getting caught because these companies protect their users' privacy and, without any moderation, on these platforms allowing Drug Trafficking Organizations the ability to evade detection.

2. What steps should Congress take to make it harder for people to market drugs to kids online?

Identify appropriate agencies or task forces for proactive operations targeting platforms and Drug Trafficking Organizations. Social media companies must actively scan for known drug terms via chat to help identify traffickers and victims.

There also needs to be the dangers of social media curriculum in all schools, including the manner of methods of drugs, child sexual abuse material, and human trafficking. These programs should be mandated at a young age and maybe even a disclaimer or warning label with every purchase or downloadable app.

Questions from Senator Tillis

for John Pizzuro, CEO of Raven

As you know, in 2021, the National Center for Missing and Exploited Children (NCMEC) cyber tipline received 29 million reports of suspected online child sexual exploitation- child sexual abuse material (CSAM). In your experience how long does it take to review each cyber tipline report?

Possible review scenarios:

- 1. Review \rightarrow no action 5-10 minutes
- 2. Review → Assignment 10-15 minutes
- 3. Review → Legal action 30 minutes

This, of course, adds no consideration for actual investigative work. Rather, this accounts for initial triage and the request for further actionable information. If you take NC, as an example they average 56 tips per day if you include weekends which amounts to 6 hours a day just reviewing the non-action ones.

Are there certain States that are receiving a higher volume of cyber tipline reports than others? If so, why are their volumes higher?

Every state has had a 100% increase year to year. The numbers are proportionate to the population of a given state. As an example, Meta is responsible for 98% of tips, and Apple is 0%, so sometimes there is a spike of tips in a certain state due to a particular service provider or VPN.

What resources and tools do our law enforcement need to efficiently and effectively review the cyber tipline reports?

Dedicated staffing and more funding to purchase technological solutions such as automation tools and Al integration. Currently, automation tools are around 300k which usually is close to the entire ICAC budget. These tools can significantly increase efficiency and reduce the backlog.

We also need help to Identify legal and technical methods to reduce exposure and/or access to children that are device-based and app-based.

Senator Sheldon Whitehouse Senate Judiciary Committee Hearing "Protecting Our Children Online" Questions for the Record for Mitch J. Prinstein Submitted February 21, 2023

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

Sec. 230 has failed to protect children. As noted in my testimony, there is evidence that some content being hosted on social media platforms is associated with mental health harms in children. APA supports the use of warning labels for adolescents. We strongly encourage platforms to take steps to prevent children from being presented with content associated with harmful impacts, especially in the event where the content is being served to children and users through automated services such as algorithms. In the absence of platforms taking action, APA believes the safe harbor under current law that protects online platforms from legal liability does not go far enough and mechanisms should be promptly put in place to protect children from the barrage of harms noted in my testimony. We are happy to discuss specific legislative and regulatory proposals that require companies to take steps to mitigate the known harms of their platforms on our children.

Judiciary Committee Hearing: Protecting Our Children Online February 14, 2023 Questions for the Record Senator Peter Welch

Questions for Dr. Mitch Prinstein

In addition to using personal devices at home, many children have access to technology in classrooms and use devices as part of standard lessons.

1. What research exists regarding how the use of technology in the classroom either positively or negatively affects students' mental health, physical health, learning outcomes, and behavior?

As with several areas of research involving the impact of technology, the findings are mixed. We have compiled the below set of resources for your review. I would be happy to meet with you and/or your staff to discuss further.

Evidence of the positive impact of technology use is widespread. (Brief list)

- Bower (2020, 2021) reports the beneficial use of technology for young children's cognitive and math learning, especially for those from under-resourced backgrounds.
 - Bower, C. A., Zimmermann, L., Verdine, B. N., Pritulsky, C., Golinkoff, R. M., & Hirsh-Pasek, K. (2021). Enhancing spatial skills of preschoolers from under-resourced backgrounds: A comparison of digital app vs. concrete materials. Developmental Science, 25(1). https://doi.org/10.1111/desc.13148
 - Bower, C., Zimmermann, L., Verdine, B., Toub, T. S., Islam, S., Foster, L., Evans, N., Odean, R., Cibischino, A., Pritulsky, C., Hirsh-Pasek, K., & Golinkoff, R. M. (2020). Piecing together the role of a spatial assembly intervention in preschoolers' spatial and mathematics learning: Influences of gesture, spatial language, and socioeconomic status. Developmental psychology, 56(4), 686–698. https://doi.org/10.1037/dev0000899
- Work conducted by Abrami and colleagues (2017) regarding early literacy and early numeracy software indicates that when used appropriately the outcomes of technology are consistently positive, with examples of international effects also evident.
 - Mak, B.S.Y., Cheung, A.C.K., Guo, X. et al. Examining the impact of the ABRACADABRA (ABRA) web-based literacy program on primary school students in Hong Kong. Educ Inf Technol 22, 2671–2691 (2017). https://doi.org/10.1007/s10639-017-9620-3
- A recent meta-analysis was conducted examining the overall effect of 36 intervention studies evaluating the effectiveness of educational apps for preschool to Grade 3 children. They found an overall significant, positive effect on students'

achievement (SD=.31) and similar effects when broken down by math and literacy (Kim et al., 2021).

- Kim, J., Gilbert, J., Yu, Q., & Gale, C. (2021). Measures Matter: A Meta-Analysis of the Effects of Educational Apps on Preschool to Grade 3 Children's Literacy and Math Skills. AERA Open, 7. https://doi.org/10.1177/23328584211004183
- When ebooks contain supportive features, such as question prompts, video links, or shared note taking with peers, evidence shows that students learn more (Clinton-Lisell et al., 2023). Moreover, the more students read, the better they will read and the more they will learn, and children are more likely to read if books interest them. Digital libraries allow for a wealth of books quickly and easily available thereby increasing the likelihood students will find books they are interested in.
 - Clinton-Lisell, Virginia & Gwozdz, Lindsey. (2023). Understanding Student Experiences of Renewable and Traditional Assignments. College Teaching. 10.1080/87567555.2023.2179591.
- "Collaborativism," refers to collaborative knowledge-building process in virtual environments (Crites et al., 2020) including virtual individual brainstorming, disagreeing, debating and considering new ideas and exploration of the merits of the differing perspectives of the group members (Harasim, 2017). Through their online discourse, students are able to interact with other cultures, points of view, and those from different socioeconomic statuses. As such, collaborativism is fundamentally a socio-cultural phenomenon influenced by cultural differences afforded by the use of technology in learning (Blau et al., 2020; Crites et al., 2020; Harasim, 2017; Stockleben et al., 2016). Such collaborativism has social, psychological, and academic benefits (Ali, 2021). For example, it positively impacts students' intellectual development in early childhood and improve their long-term educational outcomes. Socially, students enhance their social understanding and acceptance. Students show more tolerance and are open to diversity. Psychologically, students have increased self-esteem and are less anxious in the learning environment. Academically, students have more satisfaction in the learning process and feel content and satisfied. Students develop high-level skills like critical thinking, analytical thinking, synthesis, and evaluation (Ali, 2021).
 - Crites, G. E., Berry, A., Hall, E., Kay, D., Khalil, M. K., & Hurtubise, L. (2020). Applying multiple frameworks to establish effective virtual collaborative teams in academia: a review and recommendations. Medical education online, 25(1), 1742968. https://doi.org/10.1080/10872981.2020.1742968
 - Harasim, L. (2017). Learning Theory and Online Technologies (2nd ed.). Routledge. https://doi.org/10.4324/9781315716831
 - Blau, I., Shamir-Inbal, T., & Hadad, S. (2020). Digital collaborative learning in elementary and middle schools as a function of individualistic and collectivistic culture: The role of ICT coordinators' leadership experience, students' collaboration skills, and sustainability. Journal of

Computer Assisted Learning, 36(5), 672–687. https://doi.org/10.1111/jcal.12436.

- Harasim, L. (2017). Learning theory and online technologies (2nd ed.). Routledge.
- Stockleben, B., Thayne, M., Jäminki, S., Haukijärvi, I., Mavengere, N. B., Demirbilek, M., & Ruohonen, M. (2016). Towards a framework for creative online collaboration: A research on challenges and context. Education and Information Technologies, 22(2), 575–597. https://doi.org/10.1007/s10639-016-9483-z.
- Ali, H. A. (2021). The impact of a program based on collaborativist learning theory on developing EFL critical writing skills and interaction among languages and translation students. CDELT Occasional Papers in the Development of English Education, 75(1), 215–252. https://doi.org/10.21608/opde.2021.208443.
- A randomized field trial with 2,850 seventh-grade mathematics students, evaluated whether an educational technology intervention increased mathematics learning. They predicted that combining an online homework tool with teacher training could increase learning. The online tool (ASSISTments) (a) provides timely feedback and hints to students as they do homework and (b) gives teachers timely, organized information about students' work. Results showed that the intervention significantly increased student scores on an end-of-the-year standardized mathematics assessment as compared with a control group that continued with existing homework practices. Students with low prior mathematics achievement benefited most.
 - Liu, K., & Wu, J. (2021). The Effect of Online Homework (IXL) on Students' Mathematics Achievement. Asian Journal of Education and Training.
- In an examination of the effectiveness of a technology-based algebra curriculum in a wide variety of middle schools and high schools in seven states, participating schools were matched into similar pairs and randomly assigned to either continue with the current algebra curriculum for 2 years or to adopt Cognitive Tutor Algebra I (CTAI), which uses a personalized, mastery-learning, blended-learning approach. Analysis of posttest outcomes on an algebra proficiency exam finds no effects in the first year of implementation, but positive effects in the second year. The estimated effect was statistically significant for high schools but not for middle schools; in both cases, the magnitude is sufficient to improve the median student's performance by approximately eight percentile points.
 - Pane, J. F., Griffin, B. A., McCaffrey, D. F., & Karam, R. (2014). Effectiveness of Cognitive Tutor Algebra I at Scale. Educational Evaluation and Policy Analysis, 36(2), 127–144. https://doi.org/10.3102/0162373713507480.
- Karno and Hatcher (2019) utilized social cognitive theory to examine computersupported collaborative learning in early childhood. The researchers observed multiple problem-solving strategies suggesting that the collaborative learning technology enabled collective agency.

- Karno, D., & Hatcher, B. (2019). Building computer supported collaborative learning environments in early childhood classrooms. Educational Technology Research and Development. https://doi.org/10.1007/s11423-019-09686-z
- Similarly, Kuzmina and Praizendorf (2022) sought to understand how collaborative learning technologies impacted the formation of self-awareness in preschool twins. The results showed increased self-esteem, motivation for cooperation, and decreased aggressiveness and rivalry.
 - Kuzmina, A. S., & Praizendorf, E. S. (2022). Collaborative Learning Technologies in Teaching Preschool Twins. Journal of Higher Education Theory and Practice, 22(14), 123–132. https://doi.org/10.33423/jhetp.v22i14.5540.
- Schools need to understand the critical importance of a student's sense of belonging to school (the feeling of being accepted, respected and valued in the school environment McCahey et al., 2021), and that and fostering a sense of belonging can be facilitated through technology (e.g., see Allen et al., 2018). This can be critical for some groups of students (e.g., those already ostracized, socially anxious, isolated, or lonely; see review Allen et al., 2014 and Ryan et al., 2017 for early adulthood). The same strategies that foster a sense of belonging in the classroom can also foster a sense of belonging on virtual learning platforms (e.g., students feels that the teacher-student relationship is core to their sense of belonging and that they feel like they belong most when teachers show they care, are approachable, provide emotional support as well as academic support and have a good rapport them) (Allen et al., 2021).
 - Allen, K. A., Berger, E., Grove, C., Patlamazoglou, L., Gamble, N., May, F., Wurf, G., & Reupert, A. (2022). "Ask me how I am doing, be kind, and encourage me to get involved": Students' perspectives for improving belonging in secondary schools. OSF Preprints. https://doi.org/10.31219/osf.io/b4q6m
 - Allen, K. A., Ryan, T., Gray, D. L., McInerney, D., & Waters, L. (2014). Social media use and social connectedness in adolescents: The positives and the potential pitfalls. The Australian Educational and Developmental Psychologist, 31(1), 18-31. https://doi.org/10.1017/edp.2014.2
 - Geary, E., Allen, K. A., Gamble, N., & Pahlevansharif, S. (2023). Online learning during the COVID-19 pandemic: Does social connectedness and learning community predict self-determined needs and course satisfaction? Journal of University Teaching & Learning Practice, 20(1). https://ro.uow.edu.au/jutlp/vol20/iss1/13
 - Allen, K. A., Kern, M. L., Vella-Brodrick, D., Hattie, J., & Waters, L. (2018). What schools need to know about fostering school belonging: A meta-analysis. Educational Psychology Review, 30(1), 1-34. https://doi.org/10.1007/s10648-016-9389-8
 - McCahey, A., Allen, K. A., & Arslan, G. (2021). Information communication technology use and school belonging in Australian high school students. Psychology in the Schools

- In online higher education spaces as well, a sense of belonging is critical for motivation and academic outcomes and mechanisms that support belonging can include fostering autonomy and competence (e.g., Geary et al 2023)
 - Geary, E., Allen, K. A., Gamble, N., & Pahlevansharif, S. (2023). Online learning during the COVID-19 pandemic: Does social connectedness and learning community predict self-determined needs and course satisfaction? Journal of University Teaching & Learning Practice, 20(1). https://ro.uow.edu.au/jutlp/vol20/iss1/13
- Using technology to support psychological services in schools should remain an
 ongoing consideration during times where campuses become unavailable to
 physically attend (Reupert et al. 2021; 2022).
 - Reupert, A., Greenfeld, D., May, F., Berger, E., Morris, Z. A., Allen, K.-A., Summers, D., & Wurf, G. (2022). COVID-19 and Australian school psychology: Qualitative perspectives for enhancing future practice. School Psychology International, 43(3), 219–236. https://doi.org/10.1177/01430343221091953
- Even the integration of artificial intelligence and education can create new
 opportunities to vastly improve the quality of teaching and learning. Intelligent
 systems that aid in assessments, data collection, improving learning progress, and
 developing new strategies can benefit teachers. Smart tutors and asynchronous
 learning can help students achieve better learning outcomes. (Hwang et al, 2020).
 - Hwang, T. J., Rabheru, K., Peisah, C., Reichman, W., & Ikeda, M. (2020). Loneliness and social isolation during the COVID-19 pandemic. International psychogeriatrics, 32(10), 1217–1220. https://doi.org/10.1017/S1041610220000988.
- Even "gaming" gets in on the action. For example, quiz apps (that can be designed as a game) are useful and effective tools that can support the acquisition and retention of semantic knowledge in different learning settings (Ruth et al, 2021).
 - Ruth, K.S., Day, F.R., Hussain, J. et al. Genetic insights into biological mechanisms governing human ovarian ageing. Nature 596, 393–397 (2021). https://doi.org/10.1038/s41586-021-03779-7

Challenges

It is also important to point out that evidence demonstrating technologies without positive outcomes exists as well (e.g., https://detaresearch.org/research-support/no-significant-difference; Tamim, et. al.) In order to explore this phenomenon extensively, David Cohen (1987) investigated the relations between educational policy and teaching practice in instructional innovations many years ago. He recognized that Instructional practice in schools is situated in a larger organization and a longer history of academic instruction than are usually considered. Cohen concluded that rather than being a failure of technology, issues such as how technology is integrated in the classroom, teachers' familiarity with the technology, and teacher's ability to teach effectively with the technology play a significant role on how impactful the technology can be. This work clarifies the

importance of supports educators need to implement technology effectively. It is also important to note, as do Wood and colleagues (2018), that technology can work as a distraction, a challenge that has to be navigated by teachers as they learn to use technology in the classroom.

In summary, it is important therefore to note, that Institutions should not look to technologies alone for significantly improving learning outcomes. Improved learning outcomes in any classroom (in-person, online, hybrid) are the result of numerous factors (learners, curriculum, teachers, technology, materials, etc.), and thus institutional decisions must take a complex systems perspective. This is not to say the technologies are not valuable in the classroom, they are, but they are just one ingredient in a complex recipe for student success.

Citations:

- Tamim, R. M., Bernard, R. M., Borokhovski, E., Abrami, P. C., & Schmid, R. F. (2011). What forty years of research says about the impact of technology on learning: A second-order meta-analysis and validation study. Review of Educational research, 81(1), 4-28.
- Cohen, D. K. (1987). Educational Technology, Policy, and Practice. Educational Evaluation and Policy Analysis, 9(2), 153–170. https://doi.org/10.3102/01623737009002153
- Wood, E., Mirza, A., & Shaw, L. (2018) Examining On-Task and Off-Task Multitasking when Technologies Support Instruction in the Classroom, Journal of Computing in Higher Education, 30(3), 553-571;
- Wood, E., Grant, A.K., Gottardo, A., Savage, R. & Evans, M.A. (2016) Software to promote young children's growth in literacy: A comparison of online and offline formats. Early Childhood Education Research Journal, 45 (2), 207-217 DOI:10.1007/s10643-016-).
- 2. How should educational institutions consider this research when making decisions regarding technology use in classrooms?

The role of technology in the classroom is an ever evolving question as more research and newer technologies are developed. Below are some important considerations supported by research on how a teacher or educational administrator might evaluate the role of technology in the classroom.

- Fidelity to Research
 - The proliferation of technology use in education is inescapable, and generally speaking, there is broad evidence that educational technology can support many educational objectives and aims. but how educational technology is used matters. *It needs to be grounded on research-based science of learning and developmental psychology principles.* As Hirsh-Pasek et al. (2015) argue, technology use must be grounded in science-of-learning principles that need to be included for them to actually be considered "educational." Such learning experiences need to promote active, engaged, meaningful, and socially

interactive learning in order to honor the research base. Even recommended guidelines for technology build upon principles drawn directly from what we know about learning science. For example, Aguilar (2021) suggests: 1) give students "big picture" projects instead of attempting to recreate a school-like structure; 2) embrace asynchronous activities, rather than relying on synchronous experiences that may place more burdens on families; 3) focusing on ways to connect with students; 4) learn about students and their families aside from assigning learning objectives and coursework; and 5) foster opportunities for students to play in manner that encourages them to engage with ideas, foster a sense of agency or give them opportunities to be connected to others. In addition, it is essential that technology strategy choice be based on research.

- Hirsh-Pasek, K., Zosh, J. M., Golinkoff, R. M., Gray, J. H., Robb, M. B., & Kaufman, J. (2015). Putting education in "educational" apps: Lessons from the science of learning. Psychological Science in the Public Interest, 16(1), 3–34. https://doi.org/10.1177/1529100615569721.
- Aguilar, S.J., Rosenberg, J., Greenhalgh, S.P., Lishinski, A., Fütterer, T., & Fischer C. (2021). A different experience in a different moment? Teachers' social media use before and during the COVID-19 pandemic. AERA Open DOI: 10.1177/23328584211063898
- Aguilar, S.J., Galperin, H., Baek, C., & Gonzalez, E. (2021). Live instruction predicts engagement in K-12 remote learning. Educational Researcher. DOI: 10.3102/0013189X211056884 (Impact Factor: 6.39) Informed CA Assembly Bill No. 1176 (Feb 18th, 2021)
- Aguilar, S.J., Karabenick, S., Teasley, S., Baek, C. (2021). Associations between learning analytics dashboard exposure and motivation and self-regulated learning. Computers & Education. DOI: 10.1016/j.compedu.2020.104085 1:1048576

• Teacher Support

• While there is research supporting both positive and negative outcomes, the question of what impact technology use has on students depends heavily on just how interested and skilled teachers are in using it productively. That is, the impact of technology use on students depends heavily on how effectively teachers' make use of its potential. Thus, teaching training and support regarding both technical and pedagogical issues is crucial to achieving positive outcomes, issues that often do not get enough attention (Schofield, 1995; Schofield et al, 2002). Teachers should be free to define their learning goals and objectives, to use the research literature to help them select the appropriate technology to support meeting the goals, and be given opportunities to receive appropriate instruction regarding effective implementation and support especially during early acquisition.

- Schofield, J.W. (1995) Computers and Classroom Culture. Cambridge University Press, New York
- Schofield, J. W., & Davidson, A.L. (2002). Bringing the Internet to school: Lessons from an urban district. San Francisco. Jossey Bass.
- Equity

• The educational technology landscape requires educators to better attend to differences among their students with respect to both the type of technology their students have access to (e.g. tablets, laptops, desktops), and the infrastructure they have access to (e.g. high-speed internet, a quiet place to study). This requires educators to better attend to differences among their students with respect to both the type of technology their students have access to (e.g. tablets, laptops, desktops), and the infrastructure they have access to better attend to differences among their students with respect to both the type of technology their students have access to (e.g. tablets, laptops, desktops), and the infrastructure they have access to (e.g. high-speed internet, a quiet place to study).

This digital equity gap is persistent and has manifested in different ways based on which new technologies have become prevalent in educational settings. It results from a gap in understanding on the part of well-intentioned educational organizations that wish to implement novel, technology-driven approaches without sufficiently investigating what is possible within the communities they serve.

Statement for the Record

Senate Committee on the Judiciary Rosellene Bronstein February 14, 2023

Chairman Durbin, Ranking Member Grassley, Members of the Committee. My name is Rose Bronstein. I am from Chicago, Illinois. I lost my son Nate to suicide on January 13, 2022, he was just 15 years old. Nate was a warm, kind, smart child who loved playing and watching many sports, with his favorite being basketball.

Two weeks after his passing we found out that Nate had been viciously cyberbullied by over a dozen classmates at the Latin School of Chicago. This was via text and the social media platform Snapchat in the weeks leading up to his death. The text and Snapchat messaging included vicious and hateful statements, and the Snapchat "Snaps" identified Nate as the target of a message that students posted, added to and reposted until the message was broadly distributed to hundreds of Chicago-area students through the Snapchat platform. One of the messages even told Nate to "go kill yourself". Nate found the courage to report the cyberbullying to an administrator at the Latin School of Chicago, but my husband and I were never told about Nate's report of cyberbullying, despite the school's clear legal requirement to do so.

I cannot imagine the sense of isolation and anguish that my son must have felt from the cyberbullying, as well as the failures of the Latin School in the face of Nate's coming to them for help. The bullying that today's adults may have experienced or observed when growing up ended when the school bell rang. It stopped at the school doors. The cyberbullying and these harassing, menacing messages reached Nate at home, in the evening and through the weekend. Nate, like others who are the targets of social media messaging, knew and had to face that he was the unwilling center of targeted messaging spreading across Chicago area students. This is a tragically new phenomenon that no child had to deal with even just 15 years ago.

As the social media industry has grown, more and more children are suffering catastrophic harm. Carson Bride, 16 years old. Grace McComas, 15 years old. David Molak, 16 years old. These are just a few heartbreaking examples out of far, far too many children.

Beyond the individual names and faces, the research clearly supports the theory that social media has significantly increased both the scope and harm of cyberbullying. According to a recent Pew Research Survey, about 46% of U.S. teens have personally experienced cyberbullying. In our own 'Buckets Over Bullying' event in Chicago on December 12, 2022, about 43% of the youth attending self-reported being cyberbullied. Another study found that those who experienced cyberbullying were more than 4 times as likely to report thoughts of suicide and attempts. Since the emergence of social media, the suicide rate among adolescents and young adults aged 10–24 in the United States has increased an astonishing 57.4% from 2007 to 2018. All this data suggests a slow-moving, social media-fueled catastrophe having harmed and continuing to harm millions of children across our country.

To honor Nate's memory and protect other families, my husband Rob and I created a 501(c)(3) nonprofit organization called Buckets Over Bullying in honor of Nate's love of basketball. To fulfill our mission of eradicating cyberbullying in Illinois, we promote anti-cyberbullying education, advocate for new legislation, and work to increase access to legal support so that every family regardless of income can explore all options available to stop relentless, ongoing, even life-threatening cyberbullying. We have also partnered with national nonprofits, like the Organization for Social Media Safety, who, through education, technology, and advocacy fight to make social media safe for everyone.

We have accomplished much in little time, but we cannot complete the mission alone. New Federal legislation is essential to keep pace with the evolving dangers created by this new technology called social media. To protect millions of children like Nate around this country, we urgently need the following public policy updates:

Social media platforms must be held accountable. The Kids Online Safety Act would require that platforms have a duty of care to the child users they welcome, even entice, onto their platforms. To save lives, Congress must pass this legislation without delay.

Section 230 of the Federal Communications Decency Act was passed into law before social media even existed in its current form. This policy is hopelessly outdated allowing the social media industry to shield its negligence, its recklessness, and even its willful disregard of our children's safety. To save lives, Congress must reform it without delay.

Our national criminal data reporting system has not kept pace with changes in technology. While we currently receive information on crimes linked to physical addresses, crimes committed in the virtual world get reported without their website addresses. The CHATS Act would provide this desperately needed information so the public can better understand the safety of various platforms, hold them accountable, and make more informed decisions to protect families. To save lives, Congress must require more robust criminal data reporting without delay.

Congress must ensure sufficient resources for cyberbullying education in our schools and ongoing research. My son's case makes clear that cyberbullying is not well understood by the public. Students, parents, and educators may know the term "cyberbullying," but often do not fully grasp the frequency and severity of the harm or how the behavior is actually perpetrated via social media. This lack of awareness is creating unsafe learning environments, hindering educational achievement and harming students. Quite simply, it is threatening our country's future. We urgently need cyberbullying education made available in schools for students, parents, and educators, and the ongoing research to ensure such education is effective, up-todate, and evidence based. To save lives, Congress needs to appropriate sufficient funding for cyberbullying education and research without delay. Thank you again, members of this distinguished committee, for your clear interest in protecting children from the harms of social media. I hope that my son's story and the stories of others such as Carson Bride, whose mother Kristin Bride provided testimony to you, will demonstrate that these concerns are not theoretical; they are not far-off fears that have yet to materialize. Children today are suffering harm; families are being destroyed. As a mother with a broken heart, I humbly ask for your courage and resolve to stand up to Big Social and pass legislation now to save the lives of children.

####

224

U.S. Senate Committee on the Judiciary Protecting Our Children Online

Statement of Linda Charmaraman, Ph.D. Senior Research Scientist Director, Youth, Media, & Wellbeing Research Lab Wellesley Centers for Women Wellesley College

February 14, 2023

My name is Linda Charmaraman, and I am a senior research scientist at the Wellesley Centers for Women at Wellesley College. I received a Ph.D. in human development and education from UC Berkeley in 2006. I am now the director of the Youth, Media & Wellbeing Research Lab at the Wellesley Centers for Women, studying issues related to youth, the media they use, and how that media impacts their wellbeing. Much of my recent work stems from being a PI on a longitudinal grant from the National Institutes of Health that follows middle schoolers into high school, examining the risks and resiliency in early adolescents using social media. I am submitting this testimony in my personal capacity to describe what I think are some important policy directions and research findings that apply to youth, social media, and mental health.

The negative impacts of social media on youth mental health are well documented in the media: cyberbullying, poor body image, fear of missing out ("fomo"), and compulsive use that interferes with sleep. One of the very first assignments I give for the undergraduate course I teach on Social Technologies and Adolescent Development is to find the latest news stories about teen social media use. Every semester, there are countless headlines that signal an unwelcome spell that has taken over our youth or how unkind the online world can be to impressionable young minds. There might only be one article that my students can find that paints a more balanced picture.

Due to this observation, I would like to remind us of some key points that apply to this research, and research in other fields as well. We must remember that correlation does not equal causation. If in a particular study, youth who use social media are found to have more symptoms of depression, we often don't know whether those youth were more depressed to begin with. Does social media cause depression, or do depressed youth tend to use social media? Often, more in-depth, longitudinal research is needed to determine the direction of causality, that is, to find out whether the chicken or the egg came first.

For instance, there was heightened concern around the worrisome rise in depression and anxiety during the COVID-19 pandemic. Since many people also noted that there was a substantial rise in technology use for schoolchildren and record levels of downloading social media platforms such as TikTok (the #1 most downloaded app in the first quarter of 2020), many people assume that these two parallel events must not only be related to each other, but that one causes the other. In our <u>research</u> during the pandemic, we demonstrated that although there was indeed an increase in mental health difficulties and increased use of social media,

they were not statistically related to each other. In other words, there were other social factors beyond social media use that were more critical in explaining this increase in mental health struggles.

That being said, we cannot rely solely on the results of a single study to make policy decisions. This is especially the case with internal, preliminary findings and self-published materials off the internet—they are not subject to the academic standards of peer-review, therefore policy decisions should not be made based on such <u>documents</u>. In a state-of-the-field <u>review</u>, the authors concluded that there was no consensus about the impact of social media on youth mental health—that is, studies demonstrated that there were positive correlations, negative correlations, and even no relationship at all. Though individual studies can make a big splash in the media, they often have a small sample size, a non-diverse sample, or other limitations that limit the usefulness of their findings. Reporters who write about them may not have read the whole study and may not be aware of these limitations, and researchers themselves may overinflate the importance of their findings.

That's why it's important to look at the wider body of research on this topic, and to understand that this body of research does not point to one black-and-white conclusion. Many studies have nuanced findings that include both negative and positive effects of social media on youth. In today's testimony, I would like to focus on 3 key points related to this complexity.

- 1. Age restrictions on social media (e.g., COPPA) have been mainly policy decisions based on consumer protections rather than on psychological and mental wellbeing research.
- Social media can have positive effects, particularly for marginalized youth—groups like LGBTQ youth, youth of color, and others.
- 3. Youth can take an active role in using social media in a healthy way.

Let us now look at each of these key points in some more detail.

#1: Research on the effects of social media on the youngest users is scarce, and more research is needed.

The federally mandated age minimum of 13 for social media use set by COPPA originates from a governmental entity (US Federal Trade Commission) rather than from science. It stems from a need to protect children from commercial interests and collection of their personal data without their knowledge rather than from a developmental rationale.

My lab recently published one of the first <u>studies</u> on the effects of early social media initiation. We found that despite the negative press about early social media use, tweens and young teens were more frequently engaging in positive and supportive behaviors online compared to negative ones; however, if a child begins using social media (e.g., Instagram, Snapchat) at age 10 or younger, they were more likely (compared to those who started at age 13 and older) to have problematic digital behaviors, such as having online friends or joining social media sites parents would disapprove of, more unsympathetic online behaviors, and greater likelihood of online harassment and sexual harassment victimization. It's important to note that beginning social media use at age 11 or 12 wasn't significantly worse developmentally than starting at age 13. The youngest initiators were even found to have one positive benefit compared to their older

counterparts: They were more likely to engage in socially supportive and civically engaged online behaviors.

As you can see, the evidence isn't clear-cut or black-and-white about the most developmentally appropriate age to begin using social media. As mentioned before, no single study can be the solution to our problems. More longitudinal work needs to be conducted to understand the long-term benefits and challenges in diverse youth populations.

I like to think of social media onboarding as a metaphor for learning how to drive. Although adolescents tend to be more impulsive and not think ahead to future consequences as much as adults, we don't take away their ability to learn how to drive and wait for them to be more mature and ready. We provide them with guidance, practice sessions, and lessons before they go out on their own; we have laws about seat belts and texting while driving.

When it comes to social media, some of the teaching and learning happens within a "village" to help new users understand how to navigate this digital world at their fingertips. Parents are not the only ones in the family who can be an important resource—siblings, cousins, aunts and uncles can offer signposts along the journey. Social media platforms can develop <u>features</u> that nudge youth (and all users) to take breaks or reduce their exposure to negative content. Educators can incorporate the soft skills needed to thrive in a 21st century classroom. If there was a federal mandate to truly fund and welcome social media literacy and digital citizenship programs in schools across the country, I believe we could empower the next generations to be more informed users and respectful digital citizens.

#2: Social media can have positive effects, particularly for marginalized youth.

Moving beyond research from past generations that primarily focused on the cyberbullying and harassment of stigmatized individuals, social media can be particularly important for marginalized groups like LGBTQ youth, youth of color, homeless youth, and youth with intellectual or socioemotional disabilities. Online, they can have the space to develop their identities, find community that may be difficult for them to find in person, and access resources that support their wellbeing as well as opportunities for civic engagement.

For example, social media has historically served as a space where LGBTQ youth can develop their identities and find community. This can be particularly important for their mental health when there isn't a supportive in-person community available to them. In my lab's 2019 survey of over 1,000 children ages 10 to 16, we found that LGBTQ youth were more likely to join an online group in order to <u>reduce social isolation or feelings of loneliness</u>, suggesting that they were able to reach out to and engage with social media networks outside of their in-person peer circles in supportive and fortifying ways.

Social media can also provide critical resources for LGBTQ youth. They may use it to find LGBTQ spaces in their local community and to identify LGBTQ-friendly physicians. therapists, and other care providers. Finally, it can serve as a springboard for their activism. A 2013 report by the Gay, Lesbian & Straight Education Network surveying nearly 2,000 LGBTQ youth ages 13 to 18 found that 77% had taken part in an online community supporting a social cause. This signals that online spaces may be critical resources to foster civic engagement.

Similarly, youth of color—the most active users of social media—may use social media to find community and to get involved in social causes. In one study, our lab found that Black and Latinx youth aged 11-15 were more likely than white and Asian youth to join online groups that made them feel less lonely and isolated. These online communities included group chats on Snapchat, House Party, WhatsApp, and Discord, as well as groups related to things like anime fandom, sports, or hobbies.

In a <u>study of older adolescents (ages 18-25)</u>, Asian Americans reported using social media to seek support during difficult times, which is thought to be a way of navigating the stigma around mental health that reigns in many Asian cultures. Our lab is currently collaborating with Brigham and Women's Hospital in Boston on an <u>NIH-funded study</u> of how discrimination affects the mental health of Asian American adolescents, and how parents, peers, and social media can be leveraged to mitigate the negative health consequences.

For these groups and others, social media can help them build relationships, decrease loneliness, increase their self-confidence and self-esteem, and introduce them to ways to get involved in social causes. All of these things can benefit their mental health.

#3: Teens can take an active role in using social media in a healthy way.

Every summer, I teach <u>free workshops</u> for middle schoolers on how to use social media in a healthy way. In the past few years, we have focused particularly on middle school girls. Over five days, the students examine the role of technology in their lives and co-design an app to promote positive social media use. The workshops are an offshoot of my lab's <u>NIH-funded study</u> of longer-term health and wellbeing effects of social technologies, which has been ongoing since 2018.

In surveys after the 2020 workshop, girls reported increases in the importance of sharing about their abilities, achievements, and future career plans online and feeling of belonging in online communities. They also experienced significant increases in self-esteem and agency. We continue to study the effects of these workshops in order to gain a better understanding of how youth can be educated to protect themselves online.

The design of these annual workshops is informed by our lab's newly formed <u>Youth Advisory</u> <u>Board</u>, composed of middle school, high school, and college-aged youth who are former workshop attendees or co-facilitators. Their input has been incredibly valuable, and is a testament to the fact that youth should have a seat at the table—both when decisions are made about social media educational programs and when decisions are made about social media platforms they use. They are experts in their own online experiences, and can help ensure protections are effective.

Historically, the power of peer influence has typically had a negative connotation. Our recent <u>research</u> has found that despite the fact that youth turn to their parents more often than their peers about digital citizenship issues, the advice that peers give to each other was significantly more likely to have effects on later positive use of social media.

What I have found over the course of teaching this workshop is that when youth are empowered with information about how social media platforms work, and how they can use social media to their advantage rather than their detriment, they are able to take control of their experience on social media in a way that benefits their mental health and overall wellbeing—and that of their peers as well. This sector of the population has been underutilized in the UX design of social media platforms, though there has been a recent <u>uptick</u> in the importance of co-designing with youth in the industry.

Conclusion

Though social media can certainly have negative effects on youth mental health, I'd urge the Committee to recognize that it can also have positive effects. These positive effects can be particularly pronounced for marginalized youth, including LGBTQ youth, youth of color, and others. It's important to see beyond the black-and-white headlines, and to base policy decisions on the nuanced body of scientific research that is available. Not only can social media be a developmentally rich and healthy <u>resource</u> to help tweens and teens connect with others, withholding it from them (e.g., stricter age cut-offs) may even be a detriment to their mental wellbeing. Decision-making should also involve the youth who will be affected, as they have in-depth knowledge of the social media platforms they use and can bring innovative ideas to the table. There has been too much emphasis on what youth *should not* do online (e.g., risks), and very little guidance on what youth *should* do (e.g., to be resilient against risks). Together, we can create policies that protect their mental health.



February 14, 2023

Members of the Senate Judiciary Committee:

On behalf of the Coalition for a Secure & Transparent Internet (CSTI), we write in support of the Committee's upcoming hearing entitled, "Protecting Children Online" and its efforts to create a safer online experience for children and adults. CSTI is a coalition of likeminded organizations that have come together over concerns surrounding the impact of our loss of access to domain registration information, also known as WHOIS. CSTI encourages the Committee to consider the impact WHOIS has on protecting our children online.

WHOIS information is the registration data that is collected by registrars and registries at the point of registering a domain or website. This information had been publicly available since the dawn of the modern Internet and has been a valuable tool for law enforcement, cyber security investigators, child safety organizations and other third-party groups to understand *who is* behind a particular domain or website. Unfortunately, because of an overly broad interpretation of the European Union's General Data Protection Regulation (GDPR), registrars and registries are generally no longer providing this information without a court order. Without this information, cyber investigations are left without key information to remove malicious websites and prosecute the individuals behind them.

The impact of our loss of access to this information has been studied. One key collection of data is the 2021 Users Survey (links to <u>letter</u> and <u>survey</u>) conducted by <u>Messaging, Malware and <u>Mobile Anti-Abuse Working Group (M3AAWG</u>) and the <u>Anti-Phishing Working Group (APWG</u>). That survey targeted cyber investigators and anti-abuse service providers to, "determine the impact of ICANN's implementation of the EU GDPR." The survey found:</u>

"From our analysis of 277 survey responses, we find that respondents report that **changes** to WHOIS access continue to significantly impede cyber applications and forensic investigations and thus cause harm or loss to victims of phishing, malware or other cyberattacks." (emphasis added)

In addition, the survey found that:

- 94% of our respondents report that redaction [of WHOIS data] impairs their ability to investigate relationships between malicious domains and actors.
- Two-thirds of our respondents indicate that their ability to detect malicious domains has decreased.
- The solutions currently discussed at ICANN would not meet the needs of law enforcement and cybersecurity actors in terms of timelines.



Finally, Congressman Latta (R-OH) inquired with several federal agencies with investigative and prosecutorial responsibilities about the role WHOIS information played historically and the impact its loss has had on their abilities to protect consumers. Attached are responses from the Federal Trade Commission, Food & Drug Administration as well as the Department of Homeland Security.

In their responses, the FTC noted that:

"Before the GDPR took effect in May 2018, the FTC and other consumer protection and law enforcement agencies routinely relied on the publicly-available registration information about domain names in WHOIS databases to investigate wrongdoing and combat fraud. The FTC uses this information to help identify wrongdoers and their locations, halt their conduct and preserve money to return to defrauded victims."ⁱ (emphasis added)

The Department of Homeland Security's Homeland Security Investigations (HSI) responded similarly, noting:

"HSI views WHOIS information, and the accessibility to it, as critical information required to advance HSI criminal investigations, including COVID-19 fraud. Since the implementation of GDPR, HSI has recognized the lack of availability to complete WHOIS data as a significant issue that will continue to grow. If HSI had increased and timely access to registrant data, the agency would have a quicker response to criminal activity incidents and have better success in the investigative process before criminals move their activity to a different domain."ⁱⁱ (emphasis added)

In its response, HSI raises a critical point to stopping these fraudulent activities (including impersonation), and that is the need to identify all domain name registrations that are used in the perpetration of a criminal activity. Consider the study conducted by Interisle Consulting Group ("Criminal Abuse of Domain Names: Bulk Registration and Contact Information Access") which found that "cybercriminals take advantage of bulk registration services to "weaponize" large numbers of domain names for their attacks.ⁱⁱⁱ Domain name registration information, and the databases that contain that information, enable that level of analysis and give us the ability to understand how these networks are connected and deny their access before harm occurs.



The U.S. Food & Drug Administration pointed out in its response:

"Greater WHOIS access would significantly assist FDA with the identification of individuals and firms illegally selling FDA-regulated products online. WHOIS adds a layer of transparency to website, online marketplaces and vendors, and enables our regulatory cybersecurity and law enforcement personnel to link seemingly disparate websites into organized affiliated networks and track historical domain name ownership." (emphasis added)

Copies of these letters are included for your review.

As a 2019 article from SecurityTrails notes, "WHOIS records help law officers and federal government agencies investigate child pornography^{iv}..." CSTI encourages the Committee to consider the impact of WHOIS information in creating a safer online community for children and all individuals. We stand ready to work with you and your staff as you consider these important issues.

Thank you for your consideration,

The Coalition for a Secure & Transparent Internet (CSTI)

i https://secureandtransparent.org/federal-agencies-stress-important-of-whois/
 ii https://secureandtransparent.org/federal-agencies-stress-important-of-whois/
 iii https://www.interisle.net/criminaldomainabuse.html
 iv https://securitytrails.com/blog/whois-records-infosec-industry

Office of Congressional Relations

U.S. Department of Homeland Security 500 12th Street, SW Washington, DC 20536



U.S. Immigration and Customs Enforcement

July 16, 2020

The Honorable Robert E. Latta U.S. House of Representatives Washington, DC 20515

Dear Representative Latta:

Thank you for your June 24, 2020 letter to U.S. Immigration and Customs Enforcement Homeland Security Investigations (HSI) and the National Intellectual Property Rights Coordination Center (IPR Center) regarding the European Union's General Data Protection Regulation (GDPR) and its impact on HSI's ability to obtain WHOIS information in support of its criminal investigations.

HSI uses domain name registration information, previously available via online WHOIS query, to aid in the identification of persons or entities responsible for registering domains that are used to conduct a wide variety of crimes, which include intellectual property crimes, cyber-crimes (such as theft of personally identifiable information [PII] and credit card information), crimes related to illegal importation and exportation of goods, and the promotion and distribution of child sex abuse material.

HSI used WHOIS data regularly prior to the implementation of GDPR in May 2018. Subsequent to GDPR, the inability to conduct instant electronic queries has added an extra step and slowed down the investigative process. HSI continues to request and use domain name registrant information via legal process from registrars who maintain that information. The registries and registrars review requests for information and determine if the requestor has the authority, if the order was issued by a court of competent jurisdiction, and whether the request violates any portion of the GDPR. Unfortunately, there is no centralized point of contact from whom to request the information, and with over 2,000 registrars, some outside of the United States, it is sometimes difficult to determine who to contact and how to procure a legal order they will recognize and respond to. In addition to slowing the process to get registrant information, the likelihood of getting a judicial order for the release of information can be difficult since a number of requests are made in the initial stage of an investigation or response and agents may not have enough information on the criminal activity to satisfy necessary requirements. Lastly, due to the penalties that can be imposed by GDPR for improper release of a registrant's PII, many registries and registrars are redacting registrant information regardless of whether or not the subject is a citizen within the European Union.

As a recent example of GDPR inhibiting HSI investigations, the HSI Cyber Crime Center (C3) Cyber Crimes Unit identified several websites posing as legitimate coronavirus disease 2019 (COVID-19) fundraising organizations, but are actually fraudulent. These websites claim to be sites for entities such as the World Health Organization, United Nations' foundations, and other non-governmental organizations, and appear to be legitimate. When HSI conducted WHOIS queries for these domains, most of the subscriber information was redacted as a result of GDPR. Having

www.ice.gov

The Honorable Robert E. Latta Page 2

increased and expedient access to domain name registration information would have allowed HSI to identify the registered owners of the domains expeditiously in order to prevent further victimization by these illegitimate fundraising websites. When HSI is required to use legal process (e.g. administrative subpoenas, non-disclosure orders, or grand jury subpoenas) to obtain registrant information, this can cause delays and potentially negatively impact an investigation.

HSI views WHOIS information, and the accessibility to it, as critical information required to advance HSI criminal investigations, including COVID-19 fraud. Since the implementation of GDPR, HSI has recognized the lack of availability to complete WHOIS data as a significant issue that will continue to grow. If HSI had increased and timely access to registrant data, the agency would have a quicker response to criminal activity incidents and have better success in the investigative process before criminals move their activity to a different domain.

In an effort to address the challenge of limited WHOIS information as a result of GDPR, the HSI C3 has assigned full-time representatives to the Public Safety Working Group (PSWG) within the Internet Corporation for Assigned Names and Numbers (ICANN) organization. The PSWG is comprised of law enforcement and consumer protection agencies that work closely with various constituencies that are represented within the ICANN ecosystem. In the absence of a more viable solution, HSI C3 members on the PSWG continue to work with registries, domain registrars, and civil society groups to develop a consensus solution for access to domain name registration information within the ICANN framework and compliant with GDPR.

Thank you again for your letter and interest in this matter. Should you wish to discuss this matter further, please do not hesitate to contact me at (202) 732-4200.

Sincerely,

Sean Hackbarth for

Raymond Kovacic Assistant Director Office of Congressional Relations

www.ice.gov



UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION

WASHINGTON, D.C. 20580 July 30, 2020

The Honorable Robert E. Latta United States House of Representatives Washington, D.C. 20515

Dear Representative Latta:

Thank you for your June 24, 2020 letter requesting information about how the Federal Trade Commission ("FTC" or "Commission") uses domain name registration information, also known as WHOIS, to carry out its law enforcement mission, including its efforts to stop frauds related to COVID-19. You also highlighted your concerns that the implementation of the European Union's General Data Protection Regulation ("GDPR") has negatively affected the ability of law enforcement to identify bad actors online. I share your concerns about the impact of COVID-19 related fraud on consumers, as well as the availability of accurate domain name registration information.

Since the beginning of the pandemic, the FTC has been monitoring the marketplace for unsubstantiated health claims, robocalls, privacy and data security concerns, sham charities, online shopping fraud, phishing scams, work at home scams, credit scams, and fake mortgage and student loan relief schemes, and other deceptions related to the economic fallout from the COVID-19 pandemic.¹ In response, we have taken actions, including filing four cases in federal courts and sending hundreds of warning letters to businesses in the United States and abroad.² In addition, we have conducted significant public outreach and education efforts.³

Before the GDPR took effect in May 2018, the FTC and other consumer protection and law enforcement agencies routinely relied on the publicly-available registration information about domain names in WHOIS databases to investigate wrongdoing and combat fraud.⁴ The FTC uses this information to help identify wrongdoers and their locations, halt their conduct, and preserve money to return to defrauded victims. Our agencies may no longer rely on this information because, in response to the GDPR, ICANN developed new policies that significantly limit the publicly available contact information relating to domain name registrants. For

¹ See generally Prepared Statement by the Federal Trade Commission before the S. Comm. on Commerce, Science, and Transp., Subcommittee on Manufacturing, Trade, and Consumer Protection: Consumer Protection Issues Arising from the Coronavirus Pandemic (July 21, 2020), <u>https://www.ftc.gov/public-statements/2020/07/prepared-statement-federal-trade-commission-consumer-protection-issues</u>.

² See generally <u>https://www.ftc.gov/coronavirus</u>. This page is updated regularly.

³ Id.

⁴ See, e.g., Comment of the Staff of the FTC Bureau of Consumer Protection before the ICANN Public Comment Forum, In the Matter of Tentative Agreements among ICANN, U.S. Dep't of Commerce, and Network Solutions, Inc. (Oct. 29, 1999), <u>https://www.ftc.gov/policy/policy-actions/advocacy-filings/1999/10/ftc-staff-commentinternet-corporation-assigned-names; Prepared Statement of the Federal Trade Commission, Hearing on Internet Governance: The Future of ICANN, Before the Subcommittee on Trade, Tourism, and Econ. Dev. of the S. Committee on Commerce, Science, and Transp., 109th Cong. (Sept 20, 2006), <u>http://www.ftc.gov/os/testimony/P035302/governancefutureicantcommissiontestsenate09202006.pdf</u>.</u>

The Honorable Robert E. Latta - Page 2

example, before the GDPR went into effect, the FTC could quickly and easily obtain detailed information about the name, address, telephone number and email of the domain name registrant by typing a simple query. Since May 2018, however, we generally must request this information directly from the particular registrar involved. This can be a time-consuming and cumbersome process.⁵

This lack of access also limits consumers' ability to identify bad actors using WHOIS information. Prior to the GDPR, thousands of the complaints filed in our Consumer Sentinel complaint database referred to the filer's use of WHOIS data to identify businesses involved in spyware, malware, imposter scams, tech support scams, counterfeit checks, and other malicious conduct.⁶

The FTC would benefit from greater and swifter access to domain name registration data. Achieving this goal is difficult, however, given the complexity of the GDPR's effect, the required international coordination, and the many stakeholders involved. We have been working with other U.S. agencies to develop solutions through our interaction with ICANN and our international law enforcement colleagues.

One approach that could help overcome the current obstacles would be to mandate disclosure of domain name registration data associated with legal entities, as opposed to natural persons. Legal entities register a significant percentage of domain names, and the GDPR protects the information of natural persons but does not apply to information related to legal entities. ICANN's current mechanisms result in over-application of the GDPR by permitting registrars to choose whether to make the registration data of legal entities public or not. We have raised this issue within ICANN's policy development process.

I appreciate your interest in these issues. If you or your staff has additional questions or comments, please contact Jeanne Bumpus, the Director of our Office of Congressional Relations, at (202) 326-2195.

Sincerely,

sigh J. Simons

Joseph J. Simons Chairman

⁵ There are more than 2,500 ICANN accredited registrars, many located outside the U.S., with different procedures to obtain registrant data. It can be challenging to determine where to direct a request and what to include in such request for access to this now non-public information as many registrars fail to place such guidance in a location that is easy to find on their websites. After submitting a request, the FTC must wait for the registrar to approve or reject our requests. Moreover, when data is located in a foreign jurisdiction, the process may be more time consuming and require cooperation from our law enforcement partners.

⁶ In 2017, we identified over 4,000 complaints filed over a five-year-period.



August, 13, 2020

The Honorable Robert E. Latta U.S. House of Representatives Washington, DC 20515

Dear Congressman Latta:

Thank you for your letter of June 24, 2020 regarding the Coronavirus outbreak (COVID-19) and inspections. We appreciate your interest in ensuring that the Food and Drug Administration (FDA or the Agency) has the necessary tools to combat fraud and ensure the safety and supply of pharmaceuticals, human and animal food, and medical supplies. As you are aware, the U.S. Government is accelerating response efforts due to COVID-19. FDA appreciates your support, and that of Congress, as we all work together toward a united goal of controlling this outbreak.

To that end, we offer the following responses to your specific questions, broken into Criminal and Civil responses, as we have two offices that utilize WHOIS:

1. If and how your office uses or has used WHOIS in the execution of its functions?

Criminal Case Investigations

Access to WHOIS information has been a critical aspect of FDA's mission to protect public health. Implementation of the E.U. General Data Protection Regulation (GDPR) has had a detrimental impact on FDA's ability to pursue advisory and enforcement actions as well as civil and criminal relief in our efforts to protect consumers and patients.

WHOIS data has also been widely used in FDA's criminal investigations to identify individuals and organizations selling online a variety of unapproved/uncleared/unauthorized products such as opioids, counterfeit or adulterated drugs as well as purported dietary supplements containing deleterious or undeclared ingredients. Most recently, lack of WHOIS transparency significantly hindered FDA's ability to identify sellers of fraudulent and unproven treatments for COVID-19 as well as illegitimate test kits and counterfeit or substandard personal protective equipment. These cases range from a simple website marketplace to sophisticated transnational cybercrime networks involving thousands of websites, hidden servers, dark web applications and virtually linked co-conspirators. Many of these criminal conspiracies were linked or identified via historical WHOIS analysis.

FDA's ability to effectively regulate industry relies on transparency with the manufacturers and distributors of the products regulated by FDA. WHOIS data are frequently used to determine the owner or operator of particular website in the context of our regulatory duties. FDA has used WHOIS data to trace foodborne contamination or product tampering supply chains, contact website owners about illegal or deceptive

U.S. Food & Drug Administration 10903 New Hampshire Avenue Silver Spring, MD 20993 www.fda.gov

Page 2 - The Honorable Robert E. Latta

marketing or labeling online, as well as to notify online sellers about a company that has recalled products and issue Warning Letters to online sellers.

Finally, WHOIS data are an essential resource in conducting cybersecurity incident response and threat related assessments/investigations. The security and protection of FDA critical assets and infrastructure is often contingent on the identification and validation of the owners and operators of these internet resources. Specifically, the potential loss of access to WHOIS data in the cybersecurity context as part of the enforcement of GDPR would negatively impact FDA's ability to effectively analyze and validate external connections (IP addresses) within the European Union (EU).

Consistent with ICANN's (Internet Corporation for Assigned Names and Numbers) Bylaws, FDA's access to WHOIS data is essential for "the legitimate needs of law enforcement" and for "promoting consumer trust."^[1] FDA's legitimate interests are also consistent with the recitals to the GDPR, which permit processing of personal data for "preventing fraud;" "ensuring network and information security," and reporting possible "criminal acts or threats to public security" to authorities.^[2]

Civil Case Investigations

FDA's Health Fraud Branch (FDA-HFB) routinely accesses WHOIS databases to obtain information on the domain registrants for websites selling FDA-regulated commodities. FDA-HFB has a subscription to a database that also provides historical WHOIS data, as well as other data necessary to conduct internet investigations. FDA-HFB uses and has used WHOIS data to identify the recipients of warning letters, determine responsibility of FDA-regulated operations from a given domain or website, establish connections or relationships among different domains or to gather additional data points (email addresses, phone numbers, IP addresses) as part of Agency investigations.

2. If and how your office has experienced increased difficulty (including delays) in accessing WHOIS information since the May 2018 implementation of the EU GDPR?

Criminal Case Investigations

Although a small number of domestic registrars will offer WHOIS data pursuant to a written request, FDA cannot access WHOIS information without a Grand Jury subpoena, and WHOIS data is no longer available for foreign registrars. Unlike some other federal law enforcement agencies, FDA's Office of Criminal Investigations (OCI) does not have authority to issue an administrative subpoena for basic WHOIS data or WHOIS data shielded by a privacy/proxy service. Because FDA cannot access basic WHOIS data

^[1] ICANN Bylaws, Registration Directory Services Review, §4.6(e).

^[2] See GDPR Recitals 47, 49 and 50.

Page 3 - The Honorable Robert E. Latta

without a Grand Jury subpoena, which requires coordination with the Department of Justice, many investigative leads have not been sufficiently addressed or significantly hindered.

Civil Case Investigations

More often, the data in WHOIS reports in the searches that FDA-HFB is conducting are either missing, redacted or hidden via a proxy registrant for domains. This proxy service is the point of contact for any inquiries regarding the domain. There are hundreds of ICANN accredited registrars that provide proxy registrant services and in very few instances have these registrants been cooperative in providing non-public data to FDA about the owners and operators of a domain. In some cases, these proxy services refer any inquiries to the domain registrar, which provides only the publicly-available, redacted or missing WHOIS data. FDA-HFB has found that Regulation (EU) 2016/79, or GDPR, extends to domains that may not be operating strictly within the EU. In a recent example, one registrar cited the GDPR compliance requirements as the basis to broadly restrict WHOIS data, claiming the burdensome technical difficulties necessary to differentiate among customers on the basis of their likely geographic locale.

3. If and how your office would be able to more effectively conduct investigations and/or intercede in illegal activity with greater WHOIS access?

Criminal Case Investigations:

Greater WHOIS access would significantly assist FDA with the identification of individuals and firms illegally selling FDA-regulated products online. WHOIS adds a layer of transparency to websites, online marketplaces and vendors, and enables our regulatory, cybersecurity and law enforcement personnel to link seemingly disparate websites into organized affiliated networks and track historical domain name ownership.

In the past, suspects operating ecommerce websites illegally selling FDA-regulated products had to provide point of contact (POC) information. After developing sufficient probable cause, OCI agents investigating fraudsters could use this information as part of an affidavit to obtain search warrants. These search warrants often provided agents with additional investigative leads that helped identify the suspect(s), detailed information on the criminal scheme, location of ill-gotten assets and other items of value in a criminal investigation. Agents could also conduct "reverse WHOIS" searches using POC information provided by the suspects. This data has been used to link the suspect(s) to other affiliated websites. Now that WHOIS information is no longer available, it is extremely time-consuming, and in some instances not possible, for agents to fully identify the entire scope of an illicit online network.

Civil Case Investigations:

FDA-HFB would be able to quickly and efficiently identify and respond to the unlawful sales of FDA-regulated products if complete and accurate WHOIS data were available.

Page 4 - The Honorable Robert E. Latta

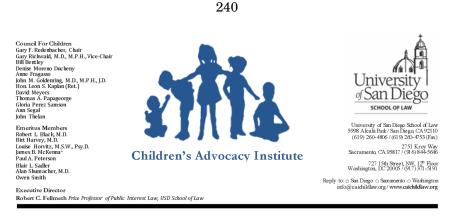
As noted above, establishing connections or determining responsibility of website owners and operators where WHOIS data are redacted or missing can be resource intensive, causing delays that can complicate investigations and cases.

Thank you again for your concern and contacting us regarding this matter. If you have any questions, please let us know.

Sincerely,

Karas Gross Karas Gross

Karas Gross Associate Commissioner for Legislative Affairs



February 12, 2023

The Honorable Dick Durbin, Chair The Honorable Lindsay Graham, Ranking Member Honorable Members United States Senate Committee on the Judiciary 224 Dirksen Senate Office Building Washington, DC 20510

Re: Social Media, The Unprecedented Child Mental Health Crisis, And The Righteous 279

Dear Chair Durbin, Ranking Member Graham, Honorable Senators:

The Children's Advocacy Institute at the University of San Diego School of Law which, for over thirty years has advanced the cause of children through academic research, legislative and regulatory advocacy, and litigation, respectfully submits this testimony as a part of the Committee's "Protecting Our Children Online" hearing, slated for February 14th.

SUMMARY OF TESTIMONY

One hundred and forty six percent. Mirroring data on child suicides, depression, and emergency room psychiatric visits, that 146% is the pre-COVID increase in the number of our young children 10 to 14 years of age who have died by their own hands using firearms during the time social media use spread widely among them.¹

Please, don't let this be just a statistic. Please, respectfully, dwell or, if you are of faith, pray on this number by imagining what childhood should be: a time of laughter, wonder, discovery.

Now, in horrifying contrast, please respectfully be intrepid enough to imagine the alone-in-their room, secreted anguish of a mere child -- capable of so much joy – as they move instead toward the dark and irrevocable decision to end their own young lives by their own small hands.

Books shelved and curricula taught in our public school libraries are subject to community preapproval. But nobody tested whether social media was safe for children before a tiny number of billion-dollar corporations employing teams of neuroscientists and computers more powerful than in science fiction unleashed it upon our children around twenty years ago. That rampant, almost utterly unregulated social media practices and technologies consumed hourly by our children is a

¹ https://everytownresearch.org/report/the-rise-of-firearm-suicide-among-young-americans/

reason we are in an utterly unprecedented child mental health crisis (one that was at red alert levels before COVID) is now not seriously disputed by anyone. Indeed, social media giants themselves know it, affirmed by their own leaked research. And as reproduced below, Open AI's ChatGPT "testifies," the paths toward a safer social media for children are well-known, requiring only the will to reform.

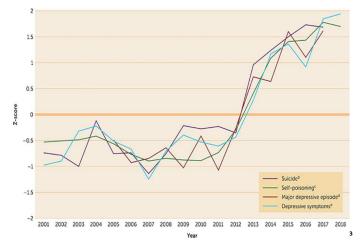
Senators, this upcoming hearing will afford you the opportunity to ask hard questions. But, with profound respect, parents, children, mental health professionals, people and communities of faith, teachers², literally everyone who cares about our children more than the profits of about five corporations would pose one question to you and your colleagues:

The Surgeon General, academic research, and the daily practice of mental health professionals repeatedly confirms that social media use among children is contributing to their unpr4ecedented suffering. Every parent knows it. Every child does, too. This will only get worse. The technology harming them now is getting better. The pressure on platforms quarterly to show market share and profit growth every quarter is unyielding. You and your colleagues are the only people in the world who can save our nation's children from terrible, documented suffering.

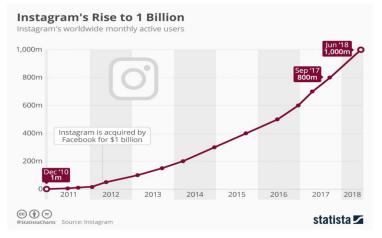
Will you?

DATA SAMPLING

Mental Health: Nobody seriously contests that we are in an unprecedented teen and youth mental crisis. Suicides, self-harm, major depression are spiking in ways never before seen, especially among teen girls.² FIGURE 1. Indicators of poor mental health among U.S. girls and young women, 2001-2018 (note, before COVID)

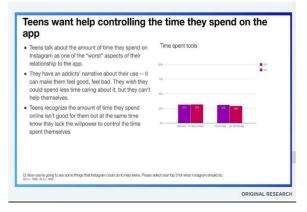


² https://www.forbes.com/sites/zacharysmith/2022/05/04/teachers-union-pushes-facebook-owner-meta-to-take-closer-look-at-harms-tochildren/?sh=3d83dd744fbd ³ https://prep.psychiatryonline.org/doi/full/10.1176/appi.prep.20190015



This never-before-seen spike in suicides among teen girls has occurred during this exact same time frame as the following:

To deny the never-before-seen child and teen mental health crisis we are currently engulfed in is at least partly the cause of social media addiction bizarrely requires denying the research conducted by the world's largest social media company about its very own operations. Here is one of the charts leaked by Frances Haugen, the former Facebook executive. Again, this is Facebook's chart documenting "an addict's narrative":



Another slide: "Among teen users [of Instagram] who reported suicidal thoughts... 6% of American [teen] users traced the desire to kill themselves to Instagram." A March 2020 presentation posted by Facebook researchers to Facebook's internal message board reported that "66% of teen girls on IG experience negative social comparison (compared to 40% of teen boys)" and that "[a]spects of Instagram exacerbate each other to create a perfect storm." "We make body

image issues worse for one in three teen girls," said one slide from 2019. "Teens blame Instagram for increases in the rate of anxiety and depression," said another slide. "This reaction was unprompted and consistent across all groups."

Research outside of Facebook's own affirms the cause-and-effect relationship between these charts. Excessive use of digital and social media has a documented relationship to increases in suicide-related outcomes in teens and children, such as suicidal ideation, plans, and attempts.⁴ Consider these findings from a 2021 U.S. Surgeon General Advisory:

- From 2009 to 2019, the proportion of high school students reporting persistent feelings of sadness or hopelessness increased by 40%;
- the share seriously considering attempting suicide increased by 36%; and
- the share creating a suicide plan increased by 44%. .
- Between 2011 and 2015, youth psychiatric visits to emergency departments for ٠ depression, anxiety, and behavioral challenges increased by 28%.
- Between 2007 and 2018, suicide rates among youth ages 10-24 in the US increased by 57%.5

During about the same period, the rates of firearm suicide among 10- to 14-year-olds in the United States increased 146%.6

In explaining the origins of this crisis, the Surgeon General noted a "growing concern about the impact of digital technologies, particularly social media, on the mental health and wellbeing of children and young people" and called for greater accountability from social media companies."7 "Business models are often built around maximizing user engagement as opposed to safeguarding users' health and ensuring that users engage with one another in safe and healthy ways. This translates to technology companies focusing on maximizing time spent, not time well spent." 8 Meanwhile, research shows reducing social media use has been shown to result in mental health benefits.9

Eating disorders. "Facebook knew Instagram was pushing girls to dangerous content: internal document" - CBS News 12.11.22 "In 2021, according to the document, an Instagram employee ran an internal investigation on eating disorders by opening a false account as a 13-year-old girl looking for diet tips. She was led to graphic content and recommendations to follow accounts titled 'skinny binge' and 'apple core anorexic.""10

Just a glance at the content pushed to girls under the secret Facebook investigation, including to girls who do not search for it, underscores the urgency of legislative action:

⁴ Elizabeth J. Ivie et al., A Meta-Analysis of the Association Between Adolescent Social Media Use and Depressive Symptoms, 275 J. of Affective Disorders 165, 165-174 (2020), https://tinyurl.com/bdzu6h8h, Alan Mozes, As Social Media Time Rises, So Does Teen Girls' Suicide Risk, U.S News (Feb. 16, 2021), https://tinvurl.com/49hzmm9v

¹⁵ U.S. SURGEON GEN, ADVISORY: PROTECTING YOU'H MENTAL HEALTH 8 (2021) at p. 25. ⁶ https://everytownresearch.org/report/the-rise-of-firearm-suicide-among-young-americans/

⁷ Id. at 25.

 ⁸ Id. (emphasis in original).
 ⁹ Roberto Mosquera et al., The Economic Effects of Facebook, 23 Exp. Econ. 575 (Jun. 2020). Melissa G. Hunt et al., No More FOMO: Limiting Cocial Media October 2010 Strength and Stren

⁴





Recently Center for Countering Digital Hate researchers set up new accounts in the United States, United Kingdom, Canada, and Australia at the minimum age TikTok allows, 13 years old. "These accounts paused briefly on videos about body image and mental health, and liked them. What we found was deeply disturbing.

Within a mere 2.6 minutes, TikTok recommended suicide content. Within 8 minutes, TikTok served content related to eating disorders. Every 39 seconds, TikTok recommended videos about body image and mental health to teens."11 Indeed, girls were delivered videos advertising breast enhancement oil and weight loss patches-without having followed any other accounts or having searched for terms related to these topics."12

As one expert observed, "Instagram perpetuates the myth that our happiness and ability to be loved are dependent on external things: For girls, it's appearance[.]"13 The picture-perfect images on Instagram's news feeds are so potent that they cement these superficial and harmful values into adolescent brains without them even knowing it."14

Sexual Abuse: Multiple investigative reports have documented how TikTok permits users to urge children to commit sexual or sexualized acts. For example, in 2022:

A Forbes review of hundreds of recent TikTok livestreams reveals how viewers regularly use the comments to urge young girls to perform acts that appear to toe the line of child pornography - rewarding those who oblige with TikTok gifts, which can be redeemed for money, or off-platform payments to Venmo, PayPal or Cash App accounts that users list in their TikTok profiles. It's 'the digital equivalent of going down the street to a strip club filled with 15-year-olds,' says Leah Plunkett, an assistant dean at Harvard Law School and faculty associate at Harvard's Berkman Klein Center for Internet & Society, focused on youth and media. Imagine a local joint putting a bunch of minors on a stage before a live adult audience that is actively giving them money to perform whatever G, PG or PG-13 activities they request, she said. "That is sexual exploitation. But that's exactly what TikTok is doing here."

As one expert observed, "[c]learly, what once was improbable [about sex trafficking and abuse of children] has been made possible through social media."15

Fentanyl Overdoses: Fentanyl was the cause of 77.14% of drug deaths among teenagers last year.16 The unprecedented spike of children dying from overdosing on fentanyl has been documented to be the fault of social media. According, for example, to The New York Times article titled "Fentanyl Tainted Pills Bought on Social Media Cause Youth Drug Deaths to Soar--Teenagers and young adults are turning to Snapchat, TikTok and other social media apps to find Percocet, Xanax and other pills. The vast majority are laced with deadly doses of fentanyl, police say?

"Law enforcement authorities say an alarming portion of [fentanyl overdoses]unfolded from counterfeit pills tainted with fentanyl that teenagers and young adults bought over social media "

https://counterhate.com/wp-content/uploads/2022/12/CCDH-Deadly-by-Design_120922.pdf
 Petition for Rulemaking to Prohibit the Use on Children of Design Features that Maximize for Engagement, Fed. Trade Comm'n (Nov. 17, 2022) at 10, https://tinyurl.com/3mursy95 Jennifer Wallace, Instagram is Even Worse than We Thought for Kids. What Do We Do about It?, WASHINGTON POST,

https://www.washingtonpost.com/lifestyle/2021/09/17/instagram-teens-parent-advice/

¹⁵ How Sex Traffickers Use Social Media to Contact, Recruit, And Sell Children, FIGHT THE NEW DRUG (Aug. 11, 2021), https://fightthenewdrug.org/how-sex-traffick.ers-use-social-media-to-contact-recruit-and-sell-children-for-sex/. (emphasis added) ¹⁶ https://www.latimes.com/califbrnia/story/2022-11-12/more-teenagers-are-dying-from -fentanyl

⁶

246

- "Social media is almost exclusively the way they get the pills," said Morgan Gire, district attorney for Placer County, Calif., where 40 people died from fentanyl poisoning last year.
- "Overdoses are now the leading cause of preventable death among people ages 18 to 45, ahead of suicide, traffic accidents and gun violence, according to federal data.
- "There are drug sellers on every major social media platform" one expert is quoted as saying...: As long as your child is on one of those platforms, they're going to have the potential to be exposed to drug sellers."



<u>Addiction</u>: "Adolescence is ... associated with an increased risk for... addictive disorders." ¹⁷ Cutting across all these harms is children being medically addicted to social media. Treating every problem associated with social media is made far harder when a child is medically addicted to a source of their mental illness. Consider these powerful excerpts from the Senate's Republican Policy Committee:

ABOUT POLICY PAPERS LEGISLATIVE NOTICES ISSUES SCHEDULE CONTACT US Q

KEY TAKEAWAYS

AN ADDICTION MACHINE

• Social media companies use artificial intelligence to determine people's interests and desires, and then they feed users content that fulfills those desires. Experts say this can be particularly problematic for adolescents, who may lack the self-discipline and maturity needed to stop watching the content.

• Research has suggested that some people experience addiction to social media in ways that are similar to addiction to drugs and other substances. ...

• One study found excessive use of social media, particularly features like "likes" and "comments," can activate release of dopamine, sometimes called the "pleasure chemical," similar to opioids or cocaine. Studies have also found scrolling through a

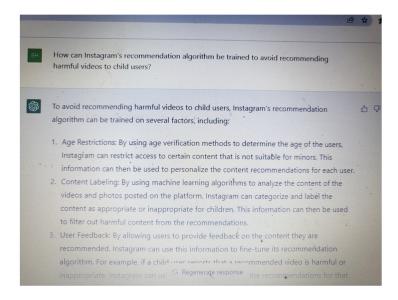
¹⁷ Christopher J. Hammond et al., Neurobiology of Adolescent Substance Use and Addictive Behaviors: Prevention and Treatment Implications, 25 ADOLESC. MED. STATE ART. REV. 15 (Apr. 2014), https://www.nebi.nlm.nih.gov/pmc/articles/PMC4446977/. ² See, e.g., the chart at the end of this letter.

⁷

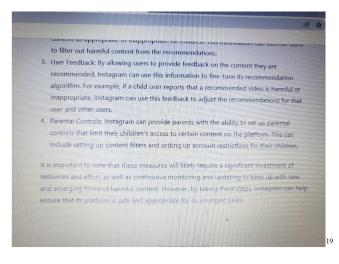
Facebook feed can produce reactions similar to those experienced through cocaine use or gambling. This addiction can have severe consequences. A decade-long study found that as the time teen girls spent on social media goes up, so does their long-term risk of suicide.

• One former Facebook executive, who quit the company and doesn't allow his children to use social media, has said, "the short-term, dopamine-driven feedback loops that we have created are destroying how society works." ... ¹⁸

ChatGPT Identifies What Can Be Done Better: AI highlights what social media platforms could do right now to make their products safer if they were required to by law. It is also what the platforms would do voluntarily if they feared -- like every other business – being held financially accountable for the foreseeable injuries they cause from the designs of their products; injuries the cost of which are now being externalized to parents, schools, health care providers – literally everyone else:



 $^{18\} https://www.rpc.senate.gov/policy-papers/social-media-and-mental-health 8$



CONCLUSION: THE RIGHTEOUS 279

The Talmud, a sacred Jewish text, refers to 36 six secret individuals for whom God preserves the world, no matter how sinful and wicked the rest of us are.²⁰ The point: a tiny handful of determinedly good people can preserve a whole planet from destruction. Without them, the world perishes.

To preserve the world of our nation's suffering children, the number is not 36. It is 279: 218 Representatives in the House, 60 of your colleagues, one Presidential signature.

Sincerely,

Small

Ed Howard, Senior Counsel, Children's Advocacy Institute

¹⁹ The full text: "How can Instagram's recommendation algorithm be trained to avoid recommending harmful videos to child users?" To avoid recommending harmful videos to child users, Instagram's recommendation algorithm can be trained on several factors, including: Age Restrictions: By using age verification methods to determine the age of the users, Instagram can restrict access to certain content that is not suitable for minors. This information can then be used to personalize the content recommendations for each user. Content Labeling: By using machine learning algorithms to analyze the content of the videos and photos posted on the platform, Instagram can categorize and label the content as appropriate or inappropriate for children. This information can then be used to filter out harmful content from the recommendations. User Feedback: By allowing users to provide feedback on the content they are recommended, Instagram can use this information to fine-tune its recommendation algorithm. For example, if a child user reports that a recommended video is harmful or inappropriate, Instagram can use this feedback to adjust the recommendations for that user and other users. Parental Controls: Instagram can provide parents with the ability to set up parental controls that limit their children's access to certain content on the platform. This can include setting up content filters and setting up account restrictions for their children. It is important to note that these measures will likely require a significant investment of resources and effort, as well as continuous monitoring and updating to keep up with new and emerging forms of harmful content. However, by taking these steps, Instagram can help ensure that its platform is safe and appropriate for its youngest users. ²⁰See, e.g., https://www.jpost.com/jewish-world/judaism/the-36-just-men-who-save-the-world-1797

Testimony for U.S. Senate Judiciary Committee Hearing Examining Kids' Online Safety

Anna Lembke, MD, Professor and Medical Director of Psychiatry and Addiction Medicine Director of the Taube Youth Addiction Initiative Stanford University School of Medicine Stanford, California February 14, 2023

Chair Durbin and Members of the Committee, thank you for your leadership in advancing this important public debate on online safety and the very real dangers of tech addiction, especially of children and transitional age youth (18-25).

I am a Professor of Psychiatry and Addiction Medicine at Stanford University School of Medicine, where I teach, do research, and see patients struggling with a range of mental health conditions including tech addiction: Addiction to digital devices and/or the digital products they deliver. In over two decades of medical practice, I have seen growing numbers of youth present with tech addiction and their downstream effects, including but not limited to anxiety, depression, suicidal ideation, insomnia, inattention, eating disorders, body dysmorphia, and the physical sequelae of physical inactivity and sleep deprivation. The types of digital products my patients are addicted to almost universally include some form of social media.

1

What is addiction? Addiction is a chronic, relapsing and remitting disease with a behavioral component, characterized by neuroadaptive brain changes resulting from exposure to addictive drugs. Every human being has the potential to become addicted. Some are more vulnerable than others. Risks for becoming addicted include genetic, developmental, and environmental factors (nature, nurture, and neighborhood). One of the biggest risk factors for addiction is simple access to addictive drugs. When supply of an addictive drug is increased, more people become addicted to and suffer the harms of that drug.

- a. The Diagnostic and Statistical Manual of Mental Disorders (DSM-5) uses the term "substance use disorder" to denote addiction. Although tech addiction is not yet included in the DSM-5, Gaming Disorder (addiction to online games) has been acknowledged by the World Health Organization and I believe the next edition of the DSM will encode tech addiction in some form.
- DSM-5 denotes 11 different criteria to diagnose opioid use disorder
 (OUD).¹ A short-hand way to remember these criteria is the "four C's":
 Control, Compulsion, Craving, and continued use despite Consequences.
 - Control refers to out-of-control use, for example using more than intended, or an inability to cut back use when necessary.

¹ Diagnostic and Statistical Manual of Mental Disorders. (DSM-5) Washington, DC: American Psychiatric Association; 2013 at p. 541.

- Compulsion refers to mental preoccupation with using against a conscious desire to abstain, and a level of automaticity that is outside conscious awareness.
- iii. Craving refers to physiologic and/or mental states of wanting.
- iv. Consequences refers to the social, legal, economic, interpersonal, and other problems that arise as a result of use, yet which still do not deter use.
- c. The DSM-5 also recognizes that addiction is a spectrum disorder, divided into mild, moderate, and severe, based on the number of criteria met.²
- From a neuroscience perspective, addiction is a disorder of the brain's reward circuitry.³
 - Digital drugs stimulate the release of the pleasure neurotransmitter dopamine in the brain's reward pathway. In order to accommodate the high amount of dopamine released, the brain adapts by downregulating its own endogenous dopamine and its own endogenous dopamine receptors. This process is called neuroadaptation, and the result is a dopamine deficit state, wherein the threshold for experiencing pleasure goes up, and the threshold for experiencing pain goes down. Addicted individuals then need

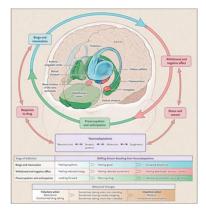
² *Id.* at pp. 541-542.

³ Koob GF, Volkow ND. Neurocircuitry of addiction. *Neuropsychopharmacology*. 2010;35:217-238. doi:10.1038/npp.2010.4.

the substance not to feel good, but to escape the pain of withdrawal.

ii. In severe forms of addiction, individuals commit all available resources to obtaining more of the substance, even forgoing natural rewards like food, finding a mate, or raising children.⁴ By hijacking the brain's reward and motivational centers, addiction leads to compulsive, self-destructive consumption that overcomes the limits of voluntary choice. The cycle of neuroadaptation is illustrated below5:

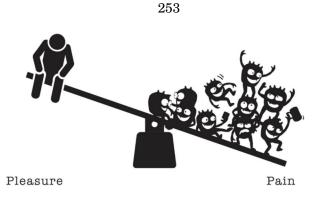
Cycle of Neuroadaptation⁶



4

⁴ Schultz W. Potential vulnerabilities of neuronal reward, risk, and decision mechanisms to addictive drugs. *Neuron*.

Schutz W. Polential vunierabilities of neuronal reward, risk, and decision mechanisms to addictive drugs. *Neurol* 2011;69(4):603-617. doi:10.1016/j.neuron.2011.02.014.
 ⁵ Volkow, ND., *et al.*, Neurobiologic Advances from the Brain Disease Model of Addiction. *N Engl J Med.* 2016; 374:363-371, Figure 1.
 ⁶ Id.



The image above⁷ is intended as a representation of the longterm effect of intoxicants, including digital drugs, on the neurocircuitry of the brain. Pleasure and pain are co-located in the brain and work like opposite sides of a balance. One of the overarching rules governing that balance is that it wants to remain level. Drugs, including digital drugs, disrupt the balance by inducing an abnormally large influx of dopamine. This results in an initial feeling of intense pleasure, followed by pain in the form of withdrawal. This is represented by the "gremlins" on the right side of the image. The addicted individual then seeks another dose of their digital drug, not to get high, but rather to avoid the pain and other negative sensations that accompany withdrawal. The universal symptoms of withdrawal from any substance or behavior are anxiety, irritability, insomnia, dysphoria, and craving. Because addiction affects the same neural pathways evolved over millions of years to encourage humans to seek out pleasure and avoid pain, everyone is vulnerable to the disease of addiction.

⁷ Lembke, Anna. *Dopamine Nation: Finding Balance in the Age of Indulgence*, 2021, Dutton Penguin Random House.

Children are especially vulnerable to neuroadaptation because their developing brains prune away the neurons and neural circuits they are using least and myelinate (make more efficient) the neural circuits they are using most. This pruning period lasts until approximately age 25, at which point the individual is left with the neural scaffolding they will use throughout their adult life.

Digital products are addictive by design. They can be analogized to cigarettes, except unlike cigarettes, digital media comes in an infinite supply available 24/7 and entirely for free. Social media is distinct from other forms of media, and distinctly more addictive, in the following ways:

- a. Social media comes in infinite supply. Quantity and frequency matter. The more of a drug a person uses, and the more often they use it, the more likely they are to get addicted to it. Social media is practically infinite and available everywhere. Most school-age children are now required to have a laptop or other device to access class schedules, grades, and lessons. In other words, these addictive platforms are woven into their everyday student life making it nearly impossible to ignore the pull of social media.
- b. Social media relies on hyper-individualized targeting. Artificial intelligence (AI) algorithms gather user-data and then use this information to suggest future digital options through targeted advertising, alerts, and push notifications. Ads, alerts, and notifications become cue-induced triggers which release dopamine in the brain's reward pathway, leading to the craving which drives continued engagement.

- c. Social media (and other platforms) use ranking, enumerations, and streaks to maintain consumer engagement. Quantification makes these digital drugs more addictive, especially when quantification becomes a way to compare to others using the same platforms. Teenagers are more sensitive to social comparitors than adults. For example, number of likes for a posted image, rankings in games, and desire to maintain 'streaks', are all ways these platforms collect and communicate numerical data to encourage compulsive overconsumption. Self-comparisons which register for the user as 'not measuring up' can lead to depression, anxiety, despair, and self-harm.
- d. Social media relies on gamblification of the platform to encourage overconsumption. Unpredictable rewards are more rewarding to the human brain than consistent rewards. The interactive nature of social media means that people are not just consuming media, they're creating and responding to it. When engagement leads to the desired and expected outcome, dopamine levels surge. When engagement leads to an undesired outcome, dopamine levels plummet. The uncertainty of the outcome is a potent elicitor of addictive behaviors, as the uncertainty of the game itself becomes the source of addiction.
- e. Social media platforms do not make it easy to de-subscribe. Parental monitoring is labor intensive and requires a level of IT sophistication that is beyond most parents. Children are good at finding ways to circumvent existing guardrails.

f. Social media is mostly free, making it more likely for consumers, especially children, to access it. The costs are largely hidden and have to do with opportunity costs (other ways children could be spending their time) and mental and physical health costs, as mentioned above.

Online digital products and devices bring with them clear societal and economic opportunities but can also lead to harms. Tech ecosystem stakeholders, including regulators, corporations, government, schools, and consumers together have a responsibility to address tech addiction and overuse, especially among youth.

Sincerely, Cum Jenk

Anna Lembke, MD



February 21, 2023

The Honorable Richard J. Durbin Chairman Senate Committee on the Judiciary 224 Dirksen Senate Office Building Washington, DC 20510 The Honorable Lindsey O. Graham Ranking Member Senate Committee on the Judiciary 224 Dirksen Senate Office Building Washington, DC 20510

Dear Chairman Durbin and Ranking Member Graham,

The Rape, Abuse & Incest National Network (RAINN) submits this statement for the record for the Senate Judiciary Committee hearing on "Protecting Our Children Online."

RAINN is the largest anti-sexual violence organization in the nation. We operate programs to prevent sexual violence, aid survivors, and ensure that perpetrators are brought to justice. In 1994 RAINN, RAINN created the National Sexual Assault Hotline (800.656.HOPE, online.rainn.org); today, RAINN's victim service programs help more than 25,000 people per month.

Since the start of the pandemic in 2020, for the first time more than half of those accessing the RAINN online hotline were children. This continues to be the case. The sexual exploitation and abuse of children has become a crisis in recent years, as offenders increasingly facilitate this exploitation through technology. According to a study from the Journal of the American Medical Association, one in six people were victims of online child sexual abuse before the age of 18. There has especially been an increase in the distribution and possession of child sexual abuse materials (CSAM). In 2022, the National Center for Missing & Exploited Children (NCMEC) received 32 million reports of CSAM to their CyberTipline, marking the highest number of reports ever received in one year. Unfortunately, thousands of child victims seen in these illicit images and videos have yet to be identified.

In addition to CSAM, an emerging form of online child sexual exploitation is sextortion. Sextortion occurs when an individual is threatened with the dissemination of sexual images/videos to coerce the individual to provide additional sexual materials. This often occurs on gaming and social media

National Sexual Assault Hotline: 800.656.HOPE | rainn.org 1220 L Street NW | Suite 500 | Washington, DC 20005 | 202-544-1034 | info@rainn.org



platforms where the predator develops relationships with children. An analysis by the Canadian Centre for Child Protection revealed that children, especially boys, are increasingly being targeted for sextortion on Instagram and Snapchat. It is apparent that the grooming and sextortion of children, and the distribution of CSAM, are occurring on online platforms. However, technology companies do not have an incentive to proactively detect, remove, and block child sexual abuse materials from their platforms nor protect children. In fact, companies are often protected by federal law, such as the Communications Decency Act Section 230, from being held accountable for illicit behavior and materials circulating on their platforms.

Congressional action is essential in ensuring children are protected online and that technology companies play an appropriate role in doing so. We, as a nation, must do better towards safeguarding children from online dangers. Therefore, RAINN recommends that the Senate Judiciary Committee prioritizes the passage of bills such as the Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act. This bill forms a commission of experts from the technology and privacy sectors, child protection and privacy advocates, and representatives from the Federal Trade Commission, U.S. Department of Justice, and the U.S. Department of Homeland Security to craft best practices and recommendations for addressing online child sexual abuse and exploitation. The bill also incentivizes technology companies to address online sexual exploitation of children by amending CDA Section 230 and allowing federal civil claims against interactive computer services, and criminal and civil enforcement of similar state statutes under existing standards.

RAINN also asks that the Senate Judiciary Committee supports the establishment of a commissioner dedicated to addressing online harms. Similar to Australia's e-Safety Commissioner, the commissioner would be responsible for addressing online harassment and creating a safer digital environment for U.S. citizens. The Commissioner would also have the authority to demand online service providers to remove seriously harmful content.

In addition, law enforcement has many obstacles in addressing the online child sexual exploitation crisis. Technology companies are required to report instances of child sexual abuse materials to the National Center for Missing & Exploited Children, CyberTipline. However, there are no requirements in what information they provide in the report. Law enforcement is inundated with inactionable CyberTipline leads that lack necessary information to investigate and pursue offenders. Therefore, they are unable to engage in proactive investigations. Additionally, due to limited resources and a lack of well-defined criteria for the prioritization of cases, it is increasingly impossible for law enforcement to keep up with the rate of children seen in these images that need to be rescued.

National Sexual Assault Hotline: 800.656.HOPE | rainn.org 1220 L Street NW | Suite 500 | Washington, DC 20005 | 202-544-1034 | info@rainn.org



We strongly encourage that the Senate Judiciary Committee directs the U.S. Department of Justice to convene a national working group of experts from the public and private sectors to study policing strategies and resources needed to rescue child victims of online sexual exploitation. We also ask that the Senate Judiciary Committee amend the Adam Walsh Child Protection and Safety Act of 2006 to ensure that law enforcement and prosecutors adopt strategies and targeting plans to prioritize the identification of offenders who commit both contact offenses and technology-facilitated crimes. We also urge the Senate Judiciary Committee to authorize funding for additional federal prosecutors dedicated to the prosecution of offenders of online child sexual exploitation.

We applaud the Senate Judiciary Committee for holding such a critical hearing and hope to see in this Congress the necessary legislation to address online harms to children, including online sexual abuse and exploitation.

Sincerely,

Suit

Scott Berkowitz President

CC: Honorable Members of the Senate Committee on the Judiciary

National Sexual Assault Hotline: 800.656.HOPE | rainn.org 1220 L Street NW | Suite 500 | Washington, DC 20005 | 202-544-1034 | info@rainn.org

February 10, 2023

To the Honorable Chair Durbin, Ranking Member Graham, and Members of the Senate Judiciary Committee.

Dear Chairman Durbin,

My name is Anastasia, I'm 18 years old, and my childhood was stolen from me when explicit videos of me being sexually abused were distributed on the internet. The trauma of having my abuse forever immortalized on the internet is something I will never be able to escape. To this day they likely are still on thousands of peoples phones. My abuser continues to roam free and traumatize other young girls.

Companies create a hyper complex process to take down content which ends up being impossible for the average adult let alone a child to navigate. Omegle, which is an app designed to connect strangers to strangers via video chat, offered an anonymous platform for my abuser to recruit other young victims. It also offered him a platform to anonymously molest children on live video. He would use tags like "One Direction" or "Hannah Montana" to directly target a young audience.

Despite countless reports to NCMEC, Reddit, Omegle, and Twitter, my abuse material continues to live and spread on the Internet. But my story is not unique. In 2022 alone, 322 million files of child sexual abuse material were found online. That number is equivalent to the entire population of the United States, but it's believed to represent only 3% of all child sexual abuse material available on the Internet.

As more and more children start using online platforms at younger ages, this number will only continue to rise. In LA County alone, we have found over 100 cases in the last year against Omegle and Kik regarding child exploitation. This issue will continue to exacerbate, as evidenced by the fact that the number of victims of online grooming tripled during the COVID-19 pandemic.

My name is Saanvi. I'm also 18 years old. Cultural differences in my family denied me the opportunity to have conversations about sexual violence at home, education which I know is disproportionately withheld from children of color. Because of this, me and so many kids like me have no idea what's going on when they unknowingly interact with predators online.

Upon getting to know each other and sharing our experiences, Ani and I decided to research the current legal grounds that allow minors to hold platforms like Omegle accountable for the abuse that they permit. It was devastating for us to learn that despite the overwhelming amount of evidence that corroborates the urgency to address this issue, there is little to no legal basis for victims of child sexual abuse to seek legal action against the platforms that permit their violence to occur. Dozens of court cases at the state level have been dismissed on these claims. Thousands of our peers have already been denied any means to hold their abuser or the platform that facilitated their abuse accountable, and millions will continue to be denied access to justice due to the dangerous precedent that current law forces our courts to set.

Every day, abusers take advantage of the features that online platforms such as Omegle, Kik, and Reddit provide under the guise of "safety;" almost all of them allow users to retain some modicum of anonymity,

making predators difficult to spot and even more difficult to track. This leaves thousands of cases unreported, as predators are given a digital curtain to hide behind. Additionally, scraping algorithms allow child sexual abuse material posted on or through these platforms to automatically get reposted to dozens of more covert websites where there is no mechanism to report content or even contact service providers to manage the material posted. This means that even if the material is removed from these larger, more mainstream platforms, the material still lives and spreads throughout the internet through more hidden channels.

This, coupled with the fact that platforms are immune to liability for facilitating child sexual abuse or distributing CSAM means that while the law explicitly prohibits the sexual abuse of or distribution of content pertaining to minors, such violence still occurs without culpable parties facing any consequences. Rather, the burden of dealing with this issue is placed on victims, who are told to "move on" without any recourse for their trauma because there are limited legal grounds for them to pursue this kind of action.

Every explicit photo of a child is a photo of a tortured child. As predators have continued to adapt to the internet, our safety measures have lagged behind. Thus, we urge you to take the necessary steps to end the injustices that 29 million survivors across the United States currently face by regulating the means through which Internet-based service providers currently profit off of child abuse.

Best, Saanvi Arora and Ani Chaglasian

ASSAULTING THE CITADEL OF SECTION 230 IMMUNITY: PRODUCTS LIABILITY, SOCIAL MEDIA, AND THE YOUTH MENTAL HEALTH CRISIS

by

Matthew P. Bergman*

The exponential rise in social media use among minors since 2008 is responsible for a precipitous increase in youth mental health injuries and suicides. These harms result from the design of social media platforms which elevate maximizing user engagement over providing minors with a safe online experience, yet social media companies benefit from broad construction of § 230 immunity to evade liability. Courts' expansive interpretation of § 230 is historically analogous to the application of the privity doctrine in the 19th century to shield manufacturers from liability for designing dangerously defective products. The demise of the privity doctrine and rise of strict product liability in the mid-20th century ameliorated the social costs of the Industrial Revolution by placing the duty of safe design on product manufacturers which resulted in safer consumer goods. Today, application of strict products liability principles to social media platforms will incentivize companies to design safer online platforms by internalizing the costs of safety within the cost of production and help reverse the mental health crisis ravaging American youth.

Introd			
I.	Social Media Harms		
II.	Th	e Emergence of Strict Products Liability	
	А.	Rise and Fall of the Privity Doctrine	
	В.	Emergence of Strict Products Liability	
		Modern Strict Products Liability	
III.	Section 230: Privity Doctrine of the Internet Age		
	А.	Origins of Section 230	
		Broad Construction of Section 230	

1159

^{*} Adjunct Professor of Law, Lewis & Clark Law School, Portland, Oregon; Founder, Social Media Victims Law Center, Seattle, Washington. Bergman currently represents parents of children who sustained mental and physical harm through their social media use in products liability litigation in state and federal courts. Special thanks go out to Professor Robert H. Klonoff and Justin Olson for their thoughtful advice, scholarship, and editorial support.

1160		LEWIS & CLARK LAW REVIEW	[Vol. 26.4	
	С.	Growing Dissent		
	D. Gonzalez v. Google: Pathway for Expanding Products Liability			
		Exception to Section 230 Immunity		
IV.	Application of Products Liability Theory to Challenge Unreasonably			
	Dai	ngerous Social Media Platforms	1190	
V.	Ass			
	А.	Social Media Platforms Are Products		
	В.	Judicial Application of Products Liability to Social Media Pl	atforms 1195	
	С.	Recent Developments in Social Media Products Liability Liti	igation . 1200	
Conclusion				

INTRODUCTION

Social media has transformed public and private life. The worldwide proliferation of social media since 2000 has had an equivalent social impact as the adoption of the printing press in the 1500s.¹ Social media usage among Americans has grown from 5% in 2005 to 72% in 2021.² Among teenagers, 95% have access to a smartphone, 95% use some form of social media, and 46% say they are online "almost constantly."[§] Social media companies have billions of subscribers⁴ and reap enormous profits, with Meta Platforms, Inc. (former Facebook) earning \$39 billion in net income in 2021.⁵

While social media has brought people together and furnished safe spaces for marginalized groups, it has also caused political polarization in societies and psychological injury among many users.⁶ Among minors, the adverse impact of social media on adolescent mental health has been well documented by academic researchers,

¹ *Compare* Bill Kovaarik, Revolutions in Communication: Media History from Gutenberg to the Digital Age (2d ed. 2016), *with* Marshall McLuhan, The Gutenberg Galaxy: The Making of Typographic Man (1962).

² Social Media Fact Sheet, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/ internet/fact-sheet/social-media/.

³ Emily A. Vogels, Risa Gelles-Watnick & Navid Massarat, *Teens, Social Media and Technology 2022*, PEW RSCH. CTR. (Aug. 10, 2022), https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/.

⁴ Felix Richter, *Meta Reaches 3.6 Billion People Each Month*, STATISTA (Oct 29, 2021), https://www.statista.com/chart/2183/facebooks-mobile-users/.

⁵ Press Release, Meta Platforms, Inc., Meta Reports Fourth Quarter and Full Year 2021 Results 1 (Feb. 2, 2022), https://s21.q4cdn.com/399680738/files/doc_financials/2021/q4/FB-12.31.2021-Exhibit-99.1-Final.pdf.

⁶ See generally Theorising Social Media, Politics and the State: An Introduction, in SOCIAL MEDIA, POLITICS AND THE STATE: PROTESTS, REVOLUTIONS, RIOTS, CRIME AND POLICING IN THE AGE OF FACEBOOK, TWITTER AND YOUTUBE 3 (Daniel Trottier & Christian Fuchs eds., 2015).

decried by legislators and regulators, and popularized through shocking disclosures by company insiders. Yet despite the nearly universal consensus that social media products are injurious to young users, social media platforms remain largely unregulated by government authorities and courts.

Section 230 of the Communications Decency Act⁷ immunizes social media providers from liability for third-party content posted on its platforms. Enacted in 1996, § 230 declares that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."⁸ In the 25 years since its enactment, courts have broadly interpreted § 230 to immunize online platforms from virtually any injury arising from social media platforms. Section 230 has been held to immunize online advertisers of child sex trafficking,⁹ platforms that match drug dealers to customers,¹⁰ and networking sites that post messages from recognized terrorist groups promoting and celebrating terrorist acts against civilians.¹¹ These decisions have erected a veritable citadel of immunity that social media companies assert protects them from virtually any legal claim for injuries in any way related to the use of their platforms.

This Article argues that products liability theory provides the most viable legal vehicle to overcome § 230 immunity, to hold social media companies legally accountable for the harm their products inflict on users, and to create economic incentives for companies to design safer platforms in the future. The Author argues that the broad immunity that social media companies currently enjoy under § 230 is historically analogous to the protection that 19th-century courts accorded to product manufacturers under the privity doctrine. Social media companies' invocation of § 230 to eschew responsibility for injuries sustained through the use of their platforms is comparable to 19th-century manufacturers' use of the privity doctrine to shield them from injury claims by consumers injured from defects in their products.

American courts' rejection of the privity doctrine in the early 20th century and subsequent adoption of strict products liability forced manufacturers to act proactively to anticipate product dangers and design safer products. By pushing manufacturers to internalize the cost of safety into the cost of production, strict products liability has, over the past 50 years, significantly enhanced the safety of consumer goods and greatly reduced serious injuries and deaths from defective products. This Article argues that courts should apply this historical example by using products

⁷ Communications Decency Act of 1996, 47 U.S.C. § 230.

⁸ Id. § 230(c)(1).

⁹ See, e.g., Doe v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016); In re Facebook, Inc., 625 S.W.3d 80 (Tex. 2021), cert. denied sub nom. Doe v. Facebook, Inc., 142 S. Ct. 1087 (2022).

¹⁰ See, e.g., Dyroff v. Ultimate Software Grp., Inc., 934 F.3d 1093 (9th Cir. 2019).

¹¹ See, e.g., Force v. Facebook, Inc., 934 F.3d 53 (2d Cir. 2019); Gonzalez v. Google LLC, 2 F.4th 871 (9th Cir. 2021).

LEWIS & CLARK LAW REVIEW

liability theory to overcome § 230 immunity and permit victims to hold social media accountable for foreseeable harms arising from defects in their platforms. The application of strict products liability will incentivize social media companies to redesign their platforms to eliminate unreasonable hazards from their platforms. Holding social media companies accountable in this manner will restore § 230 to its intended legislative purpose, force social media companies to act proactively to design safer platforms, and uphold tort law's public policy purpose of deterring negligent conduct.

I. SOCIAL MEDIA HARMS

The term "social media" refers to "a computer-based technology that facilitates the sharing of ideas, thoughts, and information through virtual networks and communities."¹² Social media provides users with instantaneous electronic communication of various types of content, including personal information, documents, videos, and photos. Users access and engage with social media through desktop computers, tablets, or (increasingly) smartphones.¹³ While widely used for socializing and entertainment, social media has also played a significant role in political expression and protest, as well as government surveillance and genocide.¹⁴

Social media use has increased exponentially over the past two decades. In 2005, Pew Research Center found that 5% of American adults used at least one social media platform.¹⁵ By 2011, that number had risen to half of all Americans, and by 2021, just over 70% of the public used some type of social media.¹⁶ Although social media is pervasive in the United States and Europe, Asian countries lead the

¹² Maya Dollarhide, *Social Media: Definition, Effects, and List of Top Apps*, INVESTOPEDIA (Aug. 31, 2021), https://www.investopedia.com/terms/s/social-media.asp.

¹³ Id.

¹⁴ See Alcides Velasquez & Hernando Rojas, Political Expression on Social Media: The Role of Communication Competence and Expected Outcomes, SOC. MEDIA + SOC'Y, Jan.-Mar. 2017, at 1– 13; Killian Clarke & Korhan Kocak, Launching Revolution: Social Media and the Egyptian Uprising's First Movers, 50 BRIT. J. POL. SCI. 1025 (2020); Jaramie D. Scott, Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space, 12 J. BUS. & TECH. L. 151 (2017); Neema Hakim, How Social Media Companies Could Be Complicit in Incitement to Genocide, 21 CHI. J. INT'L L. 83 (2020).

¹⁵ PEW RSCH. CTR., supra note 2.

¹⁶ Id.

list in social media consumption.¹⁷ As of October 2022, more than 4.7 billion people use social media.¹⁸ Among Americans, YouTube and Facebook are the most commonly used online platforms, and the demographics of their user bases are the most broadly representative of the population as a whole.¹⁹ However, younger users more frequently turn to more fast-paced platforms such as Instagram, Snapchat, and TikTok.²⁰

Social media companies employ a financial model in which consumers are not directly billed for their use of social media platforms. Instead, social media companies sell advertising on their platforms based on specific users' demographic profile and internet browsing history.²¹ Companies also sell their users' personal data to consumer product and service providers.²² Hence, the more time that users are engaged on a particular social media platform, the greater their exposure to advertising and the greater the profits earned by the particular social media platform. Unsurprisingly, like traditional television networks, social media companies seek to maximize user screen time (and exposure to advertising) by offering users attractive and interesting content. However, unlike television networks, which are subject to robust regulation by the Federal Communications Commission, social media platforms target their advertising to each individual user and operate virtually free from regulation of the content they design and publish, i.e., the means with which they attract users.²³

Bereft of regulation, social media companies have developed sophisticated computer algorithms that rely on artificial intelligence and "operant conditioning" to maximize the amount of time that users spend on their platforms.²⁴ These algo-

¹⁷ Social Media: What Countries Use It Most & What Are They Using?, DIGIT. MKTG. INST. (Nov. 2, 2021), https://digitalmarketinginstitute.com/blog/social-media-what-countries-use-itmost-and-what-are-they-using (reporting that the Philippines has the highest social media usage rate in the world).

¹⁸ *Global Social Media Statistics*, DATAREPORTAL, https://datareportal.com/social-mediausers (last visited Nov. 17, 2022).

¹⁹ PEW RSCH. CTR., supra note 2.

²⁰ Id.

²¹ Samuel M. Roth, Data Snatchers: Analyzing TikTok's Collection of Children's Data and Its Compliance with Modern Data Privacy Regulations, 22 J. HIGH TECH. L. 1, 19–22 (2021).

²² Id.

²³ Wayne Unger, *How the Poor Data Privacy Regime Contributes to Misinformation Spread and Democratic Erosion*, 22 COLUM. SCI. & TECH. L. REV. 308, 323 (2021).

²⁴ Bill Davidow, *Skinner Marketing: We're the Rats, and Facebook Likes Are the Reward*, ATLANTIC (June 10, 2013), https://www.theatlantic.com/technology/archive/2013/06/skinnermarketing-were-the-rats-and-facebook-likes-are-the-reward/276613/ (discussing B.F. Skinner's theory of operant conditioning).

rithms are individualized to each user; they anticipate the content that will be attractive to the user and are intentionally designed to be habit-forming.²⁵ As users become satiated with one type of content, the algorithms direct them to progressively more psychologically disturbing content, which triggers a greater dopamine reaction in response to the new stimuli.²⁶ Because the algorithms are designed solely to maximize user engagement, whether or not the content selected is helpful or harmful to the user is irrelevant to the social media companies. So long as users remain habituated to the social media platform, the algorithmic design is successful.

The addictive potential of social media was observed by medical professionals as early as 2009.²⁷ Subsequent research confirmed an addictive paradigm in many social media users' behavior,²⁸ particularly adolescents, and the Bergen Social Media Addiction Scale²⁹ is now widely used by researchers and mental health professionals to identify and quantify addictive social media behavior.³⁰ In November 2021, the *Wall Street Journal* revealed in The Facebook Files³¹ that Facebook, Inc.'s own internal research identified 12.5% of its users engaging in "compulsive" use of social media that impacted their sleep, work, parenting, or relationships.³² Recent reports have also demonstrated severe psychological injury and self-harm resulting from excessive social media use in all age groups.³³ However, the most impactful evidence is

³⁰ See, e.g., Chung-Ying Lin, Anders Broström, Per Nilsen, Mark D. Griffiths & Amir H. Pakpour, *Psychometric Validation of the Persian Bergen Social Media Addiction Scale Using Classic Test Theory and Rasch Models*, 6 J. BEHAV. ADDICTIONS 620 (2017).

³¹ See generally The Facebook Files, WALL ST. J., https://www.wsj.com/articles/the-facebookfiles-11631713039 (last visited Jan. 2, 2023). The Facebook Files is a compilation of *Wall Street Journal* articles describing Facebook's harms and is "based on a review of internal Facebook documents, including research reports, online employee discussions and drafts of presentations to scnior management." *Id.*

³² Georgia Wells, Deepa Seetharaman & Jeff Horwitz, *Is Facebook Bad for You? It Is for About 360 Million Users, Company Surveys Suggest*, WALL ST. J. (Nov. 5, 2011, 11:09 AM), https://www.wsj.com/articles/facebook-bad-for-you-360-million-users-say-yes-company-documents-facebook-files-11636124681?mod=hp_lead_pos7.

³³ See, e.g., Mesfin A. Bekalu, Rachel F. McCloud & K. Viswanath, Association of Social Media Use with Social Well-Being, Positive Mental Health, and Self-Rated Health: Disentangling

²⁵ See generally NIR EYAL WITH RYAN HOOVER, HOOKED: HOW TO BUILD HABIT-FORMING PRODUCTS (2014).

²⁶ Unger, supra note 23, at 323 (citing Ronald J. Deibert, *The Road to Digital Unfreedom: Three Painful Truths About Social Media*, J. DEMOCRACY, Jan. 2019, at 25, 29–30).

²⁷ See, e.g., Chih-Hung Ko, Ju-Yu Yen, Sue-Huei Chen, Ming-Jen Yang, Huang-Chi Lin & Cheng-Fang Yen, Proposed Diagnostic Criteria and the Screening and Diagnosing Tool of Internet Addiction in College Students, 50 COMPREHENSIVE PSYCHIATRY 378 (2009).

²⁸ Hunt Allcott, Matthew Gentzkow & Lena Song, *Digital Addiction* 29 (Nat'l Bureau of Econ. Rsch., Working Paper No. 28936, 2022) (finding that "self-control problems magnified by habit formation might be responsible for 31 percent of social media use").

²⁹ Cecilie Schou Andreassen, Torbjørn Torsheim, Geir Scott Brunborg & Ståle Pallesen, Development of a Facebook Addiction Scale, 110 PSYCH. REPS. 501 (2012).

the strong relationship between social media use and adverse impacts on minor users.

In December 2021, the U.S. Surgeon General issued an advisory, *Protecting Youth Mental Health*, warning of a mental health crisis among young adults caused in part by their overuse of social media.³⁴ The Centers for Disease Control reported a 146% increase in rates of suicide in the 12 to 16 age group since 2008³⁵ and a 57% increase in the 10 to 24 age group overall.³⁶ A number of authorities have noted a causal relationship between social media and teen suicide.³⁷ Moreover, the causal

³⁴ The U.S. Surgeon General found that:

In recent years, there has been growing concern about the impact of digital technologies, particularly social media, on the mental health and wellbeing of children and young people....

Importantly, the impact of technology almost certainly varies from person to person, and it also matters what technology is being used and how. So, even if technology doesn't harm young people on average, certain kinds of online activities likely do harm some young people.

U.S. SURGEON GEN., ADVISORY: PROTECTING YOUTH MENTAL HEALTH 25 (2021) (citations omitted) .

³⁵ Fatal Injury Reports, National, Regional and State, 1981–2020, CTRS. FOR DISEASE CONTROL: WEB-BASED STAT. QUERY & REPORTING SYS., https://wisqars.cdc.gov/fatal-reports (last visited Nov. 17, 2022) (for "Year Range/Census Region," select "1999 to 2020 (ICD-10), National and Regional"; for "Intent or manner of the injury," select "Suicide"; for "Cause or mechanism of the injury," select "All injury"; under "Select specific options," choose "2008" to "2020" from "Year(s) of Report" dropdowns; then under "Advanced Options," select "Custom Age Range" and choose "12" to "16" from dropdowns; then under "Select output group(s)," select "Year"; and then click "Submit Request").

³⁶ *Id.* (for "Year Range/Census Region," select "1999 to 2020 (ICD-10), National and Regional"; for "Intent or manner of the injury," select "Suicide"; for "Cause or mechanism of the injury," select "All injury"; under "Select specific options," choose "1999" to "2020" from "Year(s) of Report" dropdowns; then under "Advanced Options," select "Custom Age Range" and choose "10" to "24" from dropdowns; then under "Select output group(s)," select "Year"; and then click "Submit Request").

³⁷ See, e.g., Jean M. Twenge, A. Bell Cooper, Thomas E. Joiner, Mary E. Duffy & Sarah G. Binau, Age, Period, and Cohort Trends in Mood Disorder Indicators and Suicide-Related Outcomes in a Nationally Representative Dataset, 2005–2017, 128 J. ABNORMAL PSYCH. 185, 196–97 (2019); Rosemary Sedgwick, Sophic Epstein, Rina Dutta & Dennis Ougrin, Social Media, Internet Use and Suicide Attempts in Adolescents, 32 CURRENT OP. PSYCHIATRY 534–35, 537, 540 (2019).

Routine Use From Emotional Connection to Use, 46 HEALTH, EDUC. & BEHAV. 695 (2019) (documenting the negative health outcomes of social media use in American adults).

In these digital public spaces, which [are] privately owned and tend to be run for profit, there can be tension between what's best for the technology company and what's best for the individual user or for society. Business models are often built around maximizing user engagement as opposed to safeguarding users' health and ensuring that users engage with one another in safe and healthy ways. **This translates to technology companies focusing on maximizing time spent, not time well spent.**

LEWIS & CLARK LAW REVIEW

relationship with other severe mental health outcomes among teens has been gener-

ally accepted by behavioral health research.³⁸ The U.S. Surgeon General's advisory further reported:

From 2009 to 2019, the proportion of high school students reporting persistent feelings of sadness or hopelessness increased by 40%; the share seriously considering attempting suicide increased by 36%; and the share creating a suicide plan increased by 44%. Between 2011 and 2015, youth psychiatric visits to emergency departments for depression, anxiety, and behavioral challenges increased by 28%. Between 2007 and 2018, suicide rates among youth ages 10-24 in the US increased by 57%.³⁹

Scientists have developed various hypotheses to explain these findings.⁴⁰ Researchers on adolescent depression have described a sort of U-curve in which moderate social media usage is beneficial to adolescents, but that depression increases sharply with increased social media usage.⁴¹ Academic findings by pediatricians and psychologists were confirmed in The Facebook Files, which revealed that Meta, Inc. was aware that female users of its Instagram platform suffered from greatly increased rates of eating disorders⁴² and garnered bipartisan calls for legislative action.⁴³

The hazards of social media platforms to the mental and physical health of American youth were publicized by dramatic congressional testimony by social media CEOs and company whistleblowers.⁴⁴ The Federal Trade Commission has conducted investigations and imposed fines on Facebook, Inc. and other companies for

³⁸ See, e.g., Jean M. Twenge, Jonathan Haidt, Jimmy Lozano & Kevin M. Cummins, Specification Curve Analysis Shows that Social Media Use Is Linked to Poor Mental Health, Especially Among Girls, 224 ACTA PSYCHOLOGICA, Apr. 2022, at 8–10, Art. No. 103512.

³⁹ U.S. SURGEON GEN., *supra* note 34, at 8 (citations omitted).

⁴⁰ See Jean M. Twenge, Increases in Depression, Self-Harm, and Suicide Among U.S. Adolescents After 2012 and Links to Technology Use: Possible Mechanisms, 2 PSYCHIATRIC RSCH. CLINICAL PRAC. 19 (2020).

⁴¹ Id. at 21.

⁴² Georgia Wells, Jeff Horwitz & Deepa Seetharaman, *Facebook Knows Instagram Is Toxic* for Teen Girks, Company Documents Show, WALL ST. J. (Sept. 14, 2021, 7:59 AM), https://www. wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739?mod=hp_lead_pos7&mod=article_inline.

⁴³ Press Release, Sen. Richard Blumenthal, Blumenthal & Blackburn Introduce Comprehensive Kids' Online Safety Legislation (Feb. 16, 2022), https://www.blumenthal.senate.gov/ newsroom/press/release/blumenthal-and-blackburn-introduce-comprehensive-kids-online-safetylegislation.

⁴⁴ Protecting Kids Online: Instagram and Reforms for Young Users: Hearing Before the Subcomm. on Consumer Prot., Prod. Safety, & Data Sec. of the S. Comm. on Com., Sci., & Transp., 117th Cong. (Dec. 8, 2021) (statement of Adam Mosseri, Head of Instagram, Meta Platforms Inc.); Protecting Kids Online: Testimony from a Facebook Whistleblower: Hearing Before the S. Subcomm. on Consumer Prot., Prod. Safety, & Data Sec., 117th Cong. (Oct. 4, 2021) (statement of Frances Haugen).

data privacy breaches;⁴⁵ however, the agency currently lacks funding commensurate with the problem.⁴⁶ Similarly, several state attorney generals have filed legal actions.⁴⁷

In August 2022, the California legislature passed the California Age-Appropriate Design Code Act, explicitly requiring platforms to "prioritize the privacy, safety, and well-being of children over commercial interests" when the two conflict in cases involving users under 18.⁴⁸ The same month, the Senate Committee on Commerce, Science, and Transportation reported out the Kids Online Safety Act,⁴⁹ bipartisan legislation aimed at curbing many of the hazards posed by social media products to children.⁵⁰ While the Bill failed to garner a vote by the full Senate in the waning days of the 117th Congress, similar legislative efforts are anticipated in 2023.⁵¹ While legislative enactment and administrative enforcement may force social media companies to curb the most egregious hazards of their platforms, such efforts will do nothing to compensate victims of social media product defects and very little to create enduring economic incentives for companies to proactively research and design safer products.

II. THE EMERGENCE OF STRICT PRODUCTS LIABILITY

A. Rise and Fall of the Privity Doctrine

Justice Roger Traynor led the judicial adoption of modern products liability law, a process he described as "the transition from industrial revolution to a settled industrial society."⁵² The Industrial Revolution produced new manufacturing technologies and production methods that disrupted traditional relationships between

⁴⁵ See, e.g., Press Release, Fed. Trade Comm'n, FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/newsevents/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictionsfacebook.

⁴⁶ Hearing on Protecting Consumer Privacy Before the S. Comm. on Com., Sci., & Transp., 117th Cong. 3–5 (Sept. 29, 2021) (statement of David C. Vladeck).

⁴⁷ See, e.g., Complaint at 2, Ohio Pub. Emps. Ret. Sys. v. Meta Platforms, Inc., No. 3:21cv-08812, 2022 WL 3571995 (N.D. Cal. July 26, 2022) ("This matter arises from an egregious breach of public trust by Facebook, which knowingly exploited its most vulnerable users including children throughout the world—in order to drive corporate profits.").

⁴⁸ CAL. CIV. CODE § 1798.99.29(a), (b) (West 2022).

⁴⁹ Kids Online Safety Act, S. 3663, 117th Cong. (2022).

⁵⁰ See id.

⁵¹ Rebecca Klar, *Bills to Boost Kids' Online Safety Advance in Senate with Bipartisan Support*, HILL (July 27, 2022), https://thehill.com/policy/technology/3576234-bills-to-boost-kids-onlinesafety-advance-in-senate-with-bipartisan-support/.

⁵² Roger J. Traynor, *The Ways and Meanings of Defective Products and Strict Liability*, 32 TENN. L. REV. 363, 363 (1965).

master and servant, borrower and lender, and manufacturer and consumer.⁵⁵ As the Author has argued previously, in periods like the Industrial Revolution, when new technologies disrupt social and economic relationships, customary bonds of legal obligation must be loosened to permit social and economic change to occur.⁵⁴ During the Industrial Revolution, for example, the holistic lifetime obligations between master and servant were reduced to a circumscribed contractual relationship between the factory owner and hourly worker.⁵⁵ Similarly, 19th-century courts facilitated the growth of industry by limiting the duty of product manufacturers.⁵⁶ However, once societies absorb new technologies and define new social and economic relationships, legal systems expand to establish new legal obligations to ameliorate the social and economic disruption of technological change.⁸⁷ This process, as Traynor explained, is the "transition" that gave birth to modern products liability law.

In the field of manufacturing, this slackening of legal obligations is demonstrated in the widely followed 1842 case of *Winterbottom v. Wright.*⁵⁸ In *Winterbottom*, a coachman was severely injured by a defective stagecoach.⁵⁹ Critically, the *Winterbottom* court explicitly found all the elements of a modern products liability claim:

[T]he said mail-coach being then in a frail, weak, and infirm, and dangerous state and condition . . . and unsafe and unfit for the use and purpose aforesaid, and from no other cause, circumstance, matter or thing whatsoever, gave way and broke down, whereby the plaintiff was thrown from his seat, and in consequence of injuries then received, had become lamed for life.⁶⁰

Nevertheless, the court refused to find the coach manufacturer liable for the coachman's injuries because he had not purchased the defective stagecoach himself and therefore lacked privity of contract with the manufacturer.⁶¹

At the height of the Industrial Revolution, the *Winterbottom* judges were vitally concerned that manufacturing could not grow and prosper if manufacturers were

⁵³ See David S. Landes, The Unbound Prometheus: Technological Change and Industrial Development in Western Europe from 1750 to the Present (1969).

⁵⁴ Matthew P. Bergman, *Status, Contract, and History: A Dialectical View*, 13 CARDOZO L. REV. 171 (1991) (during periods of economic transformation, legal systems operate to limit obligations).

⁵⁵ Id. at 206–08.

⁵⁶ Traynor, *supra* note 52, at 363.

⁵⁷ Bergman, *supra* note 54, at 181.

⁵⁸ Winterbottom v. Wright (1842) 152 Eng. Rep. 402; 10 M. & W. 109.

⁵⁹ Id. at 403; 10 M. & W. at 110.

⁶⁰ Id.

⁶¹ Id. at 403; 10 M. & W. at 110-11.

obliged to compensate victims for injuries caused by their defective products.⁶² Writing for the court, Lord Abinger foresaw "the most absurd and outrageous consequences, to which I can see no limit" if a manufacturer who contracted to furnish a product to a person would be liable to a third party for its failure to produce the product in conformity with the contract.⁶⁸ Lord Alderson concurred, reasoning that "[i]f we were to hold that the plaintiff could sue in such a case, there is no point at which such actions would stop."⁶⁴ Lord Rolfe, though recognizing the harsh consequences of the court's holding, also concurred, reasoning as follows:

This is one of those unfortunate cases in which there certainly has been damnum, but it is damnum absque injuriá;⁶⁵ it is, no doubt, a hardship upon the plaintiff to be without a remedy, but by that consideration we ought not to be influenced. Hard cases, it has been frequently observed, are apt to introduce bad law.⁶⁶

Traynor tartly observed that *Winterbottom*'s holding "rested on the oft-disproved notion that wheels operate at peak efficiency when unattended by brakes."⁶⁷ Nevertheless, the contractual privity doctrine enunciated in *Winterbottom* was adopted in courts throughout the United States and effectively precluded injured plaintiffs from recovering against product manufacturers for the next 70 years.⁶⁸

Justice Benjamin Cardozo's 1916 opinion in *MacPherson v. Buick Motor Co.*⁶⁰ was the first published case to reject *Winterbottom*'s restrictive holding. In *MacPherson*, a motorist was injured when the wooden spokes on the wheels of his Buick collapsed.⁷⁰ He sued the manufacturer of the allegedly defective vehicle.⁷¹ Relying on *Winterbottom*, Buick argued that it was immune from liability because the plaintiff had purchased the automobile from through a dealer not from Buick directly; thus, under *Winterbottom*, the plaintiff lacked the contractual privity to impose liability on the manufacturer.⁷² Writing for the majority of the New York Court of Appeals, Cardozo rejected this argument, holding that if it was foreseeable that a product would be used by someone other than the direct purchaser, "then, irrespective of contract, the manufacturer of this thing of danger is under a duty to make it

⁶² Traynor, *supra* note 52, at 363–64.

⁶³ Winterbottom, 152 Eng. Rep. at 405; 10 M. & W. at 114–15.

⁶⁴ Id. at 405; 10 M. & W. at 115–16.

⁶⁵ Latin for "loss or damage without injury."

⁶⁶ Winterbottom, 152 Eng. Rep. at 405–06; 10 M. & W. at 116.

⁶⁷ Traynor, *supra* note 52, at 364.

⁶⁸ Kenneth S. Abraham, *Prosser's* The Fall of the Citadel, 100 MINN. L. REV. 1823, 1826–

^{28 (2016).}

⁶⁹ MacPherson v. Buick Motor Co., 111 N.E. 1050 (N.Y. 1916).

⁷⁰ Id. at 1051.

⁷¹ Id.

⁷² *Id.* at 1054–55.

LEWIS & CLARK LAW REVIEW

carefully."⁷³ Cardozo explicitly rejected *Winterbottom*'s holding as obsolete in light of modern economic and social life:

[T]he defendant would have us say that [the auto dealer] was the one person whom it was under a legal duty to protect. The law does not lead us to so inconsequent a conclusion. Precedents drawn from the days of travel by stage-coach do not fit the conditions of travel to-day. The principle that the danger must be imminent does not change, but the things subject to the principle do change. They are whatever the needs of life in a developing civilization require them to be.⁷⁴

In the subsequent years, Cardozo's decision "swept the country," and within a few years, almost every state had jettisoned the privity doctrine.⁷⁵

B. Emergence of Strict Products Liability

Although the court's decision in *MacPherson* marked the beginning of the end of the privity doctrine, Cardozo's reasoning did not challenge the negligence standard for proving liability. Under the negligence theory, it was not sufficient that plaintiffs prove that their injuries resulted from a design defect that rendered the manufacturer's product unreasonably dangerous. Rather, the plaintiff had to prove that the manufacturer knew, or in the exercise of reasonable care should have known, that its product was hazardous to ordinary users and nevertheless failed to take reasonable steps to ameliorate this hazard.⁷⁶ And while *MacPherson* inspired state courts throughout the country to reject the privity doctrine as a shield to manufacturer's liability, actually proving that a manufacture knew or should have known its product was defective remained a near-insurmountable barrier through the first half of the 20th century.

The concept of strict products liability was first promoted in academic circles by Professor Karl Llewellyn in the 1930s.⁷⁷ However, no jurist adopted the doctrine

⁷⁶ See, e.g., Lockwood v. AC & S, Inc., 744 P.2d 605, 615 (Wash. 1987). In *Lockwood*, the court approved the following jury instruction pertaining to negligence: "A manufacturer's duty to exercise ordinary care is bounded by the foreseeable range of danger. In order to recover on the theory of negligence, plaintiff must prove that the defendant should have anticipated an unreasonable risk of danger to him or to other workers of his class." *Id.* app. at 624.

⁷⁷ See KARL N. LLEWELLYN, CASES AND MATERIALS ON THE LAW OF SALES (1930); K.N. Llewellyn, On Warranty of Quality, and Society, 36 COLUM. L. REV. 699, 744, 704 n.14 (1936); see also John B. Clutterbuck, Note, Karl Llewellyn and the Intellectual Foundations of Enterprise Liability Theory, 97 YALE LJ. 1131 (1988).

⁷³ Id. at 1053.

⁷⁴ Id.

⁷⁵ William L. Prosser, *The Assault Upon the Citadel (Strict Liability to the Consumer)*, 69 YALE LJ. 1099, 1100–02 (1960) ("During the succeeding years this decision swept the country, and with the barely possible but highly unlikely exceptions of Mississippi and Virginia, no American jurisdiction now refuses to accept it.").

until Traynor's 1944 concurrence in *Escola v. Coca Cola Bottling Co.*⁷⁸ The Supreme Court of California laid out the facts in *Escola* as follows:

Plaintiff, a waitress in a restaurant, was injured when a bottle of Coca Cola broke in her hand. She alleged that defendant company, which had bottled and delivered the alleged defective bottle to her employer, was negligent in selling "bottles containing said beverage which on account of excessive pressure of gas or by reason of some defect in the bottle was dangerous . . . and likely to explode."⁷⁹

The jury found for the plaintiff, and the manufacturer appealed.⁸⁰ The Supreme Court of California affirmed, finding that the evidence supported a reasonable inference that the bottle had not been damaged after delivery, but rather it was in some manner defective at the time the defendant relinquished control "because sound and properly prepared bottles of carbonated liquids do not ordinarily explode when carefully handled."⁸¹

Traynor concurred in the judgment but wrote separately to posit for the first time that "the manufacturer's negligence should no longer be singled out as the basis of a plaintiff's right to recover."⁸² Instead, Traynor argued that "it should now be recognized that a manufacturer incurs an absolute liability when an article that he has placed on the market, knowing that it is to be used without inspection, proves to have a defect that causes injury to human beings."⁸³ Rejecting negligence as the sole basis for the manufacturer's liability, Traynor reasoned:

[P]ublic policy demands that responsibility be fixed wherever it will most effectively reduce the hazards to life and health inherent in defective products that reach the market. It is evident that the manufacturer can anticipate some hazards and guard against the recurrence of others, as the public cannot. Those who suffer injury from defective products are unprepared to meet its consequences. The cost of an injury and the loss of time or health may be an overwhelming misfortune to the person injured, and a needless one, for the risk of injury can be insured by the manufacturer and distributed among the public as a cost of doing business. . . . Against such a risk there should be general and constant protection and the manufacturer is best situated to afford such protection.⁸⁴

⁷⁸ Escola v. Coca Cola Bottling Co., 150 P.2d 436, 440–44 (Cal. 1944) (Traynor, J., concurring).

⁷⁹ Id. at 437 (majority opinion).

⁸⁰ Id.

⁸¹ Id. at 439.

⁸² Id. at 440 (Traynor, J., concurring).

⁸³ Id.

⁸⁴ Id. at 440-41.

LEWIS & CLARK LAW REVIEW

Professor Keith Hylton observes that Traynor's concurring opinion in Escola articulated the public policy rational for strict products liability: deterrence, reliance, insurance, and administrative costs.85 The deterrence rationale posits that "strict products liability provides an incentive for the party best able to control product accidents to take steps to minimize their occurrence."86 This presupposes that consumers are unable to accurately evaluate the level of risk presented by a specific product and that, in the absence of strict liability, manufacturers will not undertake sufficient care.⁸⁷ Relatedly, the reliance rationale posits that strict products liability is more appropriate than negligence under modern production and marketing because consumers rely on the assurances of manufacturers.⁸⁸ The insurance rationale provides that "strict products liability is desirable because it spreads the risks of injuries caused by defective products."89 This theory posits that, because consumers have limited information to distinguish between safe and unsafe products, through strict products liability they, in effect, purchase an insurance policy along with the product.⁹⁰ As Judge Richard Posner explains, "Strict liability in effect impounds information about product hazards into the price of the product, resulting in a substitution away from hazardous products by consumers who may be completely unaware of the hazards."91 Finally, the administrative costs rationale provides that strict products liability achieves the same objectives as negligence but does so in a more efficient fashion.92

Although Traynor's concurrence in *Escola* articulated the intellectual basis for modern products liability law, "its largest immediate impact [was] in the arena of ideas rather than in the case law."⁹³ Despite his lack of judicial followers, Traynor's reasoning was widely promoted by Berkley Law School Dean William Prosser in his 1960 article *The Assault Upon the Citadel*,⁹⁴ as well as by other scholars advocating for a more modern concept of strict liability. Prosser's *Assault Upon the Citadel* remains one of the most frequently cited law articles in history.⁹⁵ In it, he discussed the rationale of strict liability over negligence:

1172

⁹¹ RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW § 6.6, at 166 (3d ed. 1986).

⁸⁵ Keith N. Hylton, *The Law and Economics of Products Liability*, 88 NOTRE DAME L. REV. 2457, 2463 (2013).

⁸⁶ Id.

⁸⁷ Id. at 2465.

⁸⁸ Id.

⁸⁹ Id. at 2465–66.

⁹⁰ Id. at 2466.

⁹² Hylton, *supra* note 85, at 2466.

⁹³ Id.; Robert E. Keeton, In Tribute to Roger Traynor, 2 HOFSTRA L. REV. 451, 453–54 (1974).

⁹⁴ Prosser, *supra* note 75, at 1120.

⁹⁵ Fred R. Shapiro, *The Most-Cited Articles from* The Yale Law Journal, 100 YALE L.J. 1449, 1470–71 (1991); Abraham, *supra* note 68, at 1833–34.

The public interest in human life, health and safety demands the maximum possible protection that the law can give against dangerous defects in products which consumers must buy, and against which they are helpless to protect themselves; and it justifies the imposition, upon all suppliers of such products, of full responsibility for the harm they cause, even though the supplier has not been negligent... The supplier, by placing the goods upon the market, represents to the public that they are suitable and safe for use; and by packaging, advertising or otherwise, he does everything that he can to induce that belief. He intends and expects that the product will be purchased and used in reliance upon this assurance of safety; and it is in fact so purchased and used.⁹⁶

Prosser's observation that "[t]he assault upon the citadel of privity is proceeding in these days apace"⁹⁷ proved prescient because the same year the New Jersey Supreme Court in *Henningsen v. Bloomfield Motors, Inc.*⁹⁸ became the first court to adopt strict products liability. *Henningsen* involved injuries from a single car accident, with evidence that the accident was caused by a defect in the steering mechanism.⁹⁹ The court expressly embraced Traynor's goal of internalizing the cost of safety to the manufacturer such that "the burden of losses consequent upon the use of defective articles is borne by those who are in a position to either control the danger or make an equitable distribution of the losses when they do occur."¹⁰⁰ Following Cardozo's mandate that tort law must adapt to contemporary economic reality, the court held that strict liability was necessary to protect consumers from defective products:

Under modern conditions the ordinary layman, on responding to the importuning of colorful advertising, has neither the opportunity nor the capacity to inspect or to determine the fitness of an automobile for use; he must rely on the manufacturer who has control of its construction

Accordingly, we hold that under modern marketing conditions, when a manufacturer puts a new automobile in the stream of trade and promotes its purchase by the public, an implied warranty that it is reasonably suitable for use as such accompanies it into the hands of the ultimate purchaser.¹⁰¹

. . . .

⁹⁶ Prosser, *supra* note 75, at 1122–23.

⁹⁷ Id. at 1099 (quoting Ultramares Corp. v. Touche, 174 N.E. 441, 445 (N.Y. 1931)).

⁹⁸ Henningsen v. Bloomfield Motors, Inc., 161 A.2d 69 (N.J. 1960); see William L. Prosser, The Fall of the Citadel (Strict Liability to the Consumer), 50 MINN. L. REV. 791, 793–94 (1966).

⁹⁹ Henningsen, 161 A.2d at 75.

¹⁰⁰ Id. at 81.

¹⁰¹ Id. at 83-84.

LEWIS & CLARK LAW REVIEW Three years later, in Greenman v. Yuba Power Products, Inc., 102 Traynor, having

recently been elevated to chief justice, adopted his reasoning in Escola as the opinion of the full court. Writing for the court, Traynor held:

To establish the manufacturer's liability it was sufficient that plaintiff proved that he was injured while using the [product] in a way it was intended to be used as a result of a defect in design and manufacture of which plaintiff was not aware that made the [product] unsafe for its intended use.¹⁰

In advancing the public policy justifications for strict products liability, Traynor's opinion made multiple citations to Prosser's Assault on the Citadel.¹⁰⁴

In his 1966 article The Fall of the Citadel (Strict Liability to the Consumer),¹⁰⁵ Prosser characterized Henningsen and Greenman as "twin landmarks" of "the most rapid and altogether spectacular overturn of an established rule in the entire history of the law of torts."106 However, Prosser's influence on the rise of strict products liability extended far beyond the role of an academic spectator. As the sole reporter for the American Law Institute's Restatement (Second) of Torts, Prosser sought to shape the emerging products liability jurisprudence to encompass the arguments he had been advancing for decades.¹⁰⁷ Indeed, critics have even charged that Prosser's promulgation of § 402A was not so much a restatement of the existing law as advancing new law.¹⁰⁸

Traynor's influence also extended beyond authoring opinions; he served as an advisor to the American Law Institute.¹⁰⁹ From the mid-1950s to the mid-1960s, Prosser, Traynor, and other luminaries had gathered for biannual three-day sessions of deliberations over all issues in the field of torts.¹¹⁰ Prosser and Traynor's collaboration culminated in 1965 when the American Law Institute approved and adopted a new section in the Restatement (Second) of Torts providing for strict liability untethered to the concept of "warranty."111 Section 402A represented the first effort at a general statement of products liability law.¹¹²

¹⁰² Greenman v. Yuba Power Prods., Inc., 377 P.2d 897 (Cal. 1963).

¹⁰³ Id. at 901.

¹⁰⁴ See id. at 900–01 (citing Prosser, supra note 75, at 1124–34).

¹⁰⁵ Prosser, supra note 98.

¹⁰⁶ Id. at 793–94, 803.

¹⁰⁷ Abraham, *supra* note 68, at 1835–36.

¹⁰⁸ See. e.g., George L. Priest, The Invention of Enterprise Liability: A Critical History of the Intellectual Foundations of Modern Tort Law, 14 J. LEGAL STUD. 461, 514 (1985).

¹⁰⁹ *Id.* at 512.

¹¹⁰ Keeton, *supra* note 93, at 451.

¹¹¹ Restatement (Second) of Torts § 402A cmt. m (Am. L. Inst. 1965).

¹¹² See James A. Henderson, Jr. & Aaron D. Twerski, A Proposed Revision of Section 402A of the Restatement (Second) of Torts, 77 CORNELL L. REV. 1512, 1526-27 (1992).

402 A. Special Liability of Seller of Product for Physical Harm to User or Consumer

(1) One who sells any product in a defective condition unreasonably dangerous to the user or consumer or to his property is subject to liability for physical harm thereby caused to the ultimate user or consumer, or to his property, if

(a) the seller is engaged in the business of selling such a product, and

(b) it is expected to and does reach the user or consumer without substantial change in the condition in which it is sold.

(2) The rule stated in Subsection (1) applies although

(a) the seller has exercised all possible care in the preparation and sale of his product, and

(b) the user or consumer has not bought the product from or entered into any contractual relation with the seller. $^{\rm 113}$

Henningsen, Greenman, and the *Restatement* were influential in persuading courts around the country to reject the privity doctrine and impose strict liability for defective product sellers.¹¹⁴ Today, most states have adopted § 402A, or a doctrine of strict products liability similar to that proposed in § 402A.¹¹⁵

C. Modern Strict Products Liability

The late 1970s marked the high-water mark of strict products liability. While the concept of strict liability to manufacturers of defective products was generally accepted, business and insurance groups resisted the imposition of strict liability on product sellers who were not involved in the manufacturing process.¹¹⁶ Manufacturers also complained of the inconsistent interpretation of § 402A among state

¹¹³ Restatement (Second) of Torts § 402A.

¹¹⁴ Abraham, *supra* note 68, at 1833–34.

¹¹⁵ By 1978, 31 states had adopted § 402A. Roger Dean Graham, *Products Liability and Tort Risk Distribution in Government Contract Programs*, 20 A.F. L. REV. 331, 342 (1978). As of 2021, "Most states have adopted the products liability approach recommended in the Restatement (Second), Torts § 402A." Cecilia Plaza, *Cutting Out the Middleman: Empirically Testing the Continued Applicability of the Learned Intermediary Rule in the Age of Direct-to-Consumer Advertising of Prescription Pharmaceuticals*, 24 QUINNIPIAC HEALTH L.J. 393, 399 (2021); see also infra text accompanying notes 119–21.

¹¹⁶ See CONG. RSCH. SERV., R40148, PRODUCTS LIABILITY: A LEGAL OVERVIEW 13 (2014); Victor E. Schwartz & Mark A. Behrens, *The Road to Federal Products Liability Reform*, 55 MD. L. REV. 1363, 1365, 1373 (1996) (discussing the work of a federal task force, advocacy groups, and "scores of small business owners" in pushing for federal products liability reform).

courts.¹¹⁷ In 1979, the Department of Commerce issued the Model Uniform Product Liability Act (UPLA) to resolve uncertainties in the tort litigation system.¹¹⁸ The most controversial aspect of products liability litigation had been the issue of defining the basic standards of responsibility to which product manufacturers are to be held. Section 402A focuses primarily on manufacturing defects and not on defects concerning design or the duty to warn. The UPLA sought to dispel some of this confusion by setting forth express criteria relating to the basic standards of responsibility to be imposed on manufacturers of a defective product. The UPLA provides that strict liability may be imposed when:

(A) The product was unreasonably unsafe in construction;

(B) The product was unreasonably unsafe in design;

1176

(C) The product was unreasonably unsafe because adequate warnings or instructions were not provided; [or]

(D) The product was unreasonably unsafe because it did not conform to an express warranty. $^{\scriptstyle 119}$

By the mid-to-late 1980s, at least 16 state legislatures had replaced common law products liability under § 402A with express products liability statutes.¹²⁰ Most of these statutes were based on the UPLA,¹²¹ while some states simply codified § 402A.¹²² The UPLA curtailed the wide liability conferred by § 402A, generally relieving product sellers of the strict liability restricted to manufacturers. The UPLA also added a risk–utility test to determine product defects. However, while most states no longer impose strict liability on product sellers, strict liability on product manufacturers is firmly entrenched in our jurisprudence and adopted by common law or statute in all 50 states.¹²³

¹¹⁷ See Sydney Knell Leavitt, Death by Chicken: The Changing Face of Allergy Awareness in Restaurants and What to Do When Food Bites Back, 42 U. TOL. L. REV. 963, 969 (2011).

¹¹⁸ Model Uniform Product Liability Act, 44 Fed. Reg. 62,714, 62,714 (Oct. 31, 1979); Connie Kemp Jobe, *The Model Uniform Product Liability Act: Basic Standards of Responsibility for Manufacturers*, 46 J. AIR L. & COM. 389, 389–90, 417 (1981).

¹¹⁹ Model Uniform Product Liability Act, 44 Fed. Reg. at 62,721.

¹²⁰ Fairfax Leary, Jr. & David Frisch, Uniform Commercial Code Annual Survey: General Provisions, Sales, Bulk Transfers, and Documents of Title, 39 BUS. LAW. (ABA) 1851, 1869 n.77 (1984) (citing Williams v. W. Penn Power Co., 467 A.2d 811, 817 n.18 (Pa. 1983)).

¹²¹ See, e.g., Philip A. Talmadge, *Washington's Product Liability Act*, 5 U. PUGET SOUND L. REV. 1 (1981) (analyzing the state of Washington's Tort and Product Liability Reform Act, which was modeled after the UPLA).

¹²² See, e.g., OR. REV. STAT. § 30.920 (2021) ("It is the intent of the Legislative Assembly that . . . this section shall be construed in accordance with the Restatement (Second) of Torts sec. 402A, Comments a to m (1965).").

¹²³ See PRODUCT LIABILITY DESK REFERENCE: A FIFTY-STATE COMPENDIUM (Morton F. Daller & Nicholas G. Daller eds., 2022).

Modern products liability has three bases on which liability may be imposed: design defect, manufacturing defect, and failure to warn. The design defect theory "asserts that the manufacturer's design is itself unreasonably dangerous."¹²⁴ Courts have applied two tests to evaluate design defects claims: the "consumer expectations" test and the "risk–utility" test. Under the consumer expectations test, the plaintiff must prove "that the product failed to conform to the safety expectations of the ordinary consumer."¹²⁵ Under the risk–utility test, the plaintiff must prove that the reduction in accidents resulting from an alternative design far exceeds the cost associated with implementing the alternative design.¹²⁶ A manufacturing defect, on the other hand, results from an error specifically in the fabrication process, as distinct from an error in the design process.¹²⁷

Even if a product suffers neither a manufacturing nor design defect, a manufacturer still may be strictly liable under a failure to warn theory.¹²⁸ Under the UPLA, a product may be defective if it failed to contain adequate instructions or warnings regarding the dangers and safe use of the product, considering the characteristics of the product, and ordinary customer knowledge of a consumer who purchases the product.¹²⁹ Courts have found defendants liable "where the burden of providing a warning is less than the foreseeable harms to the consumer."¹³⁰

Thirty years after the adoption of the Model Product Liability Act, which curtailed strict liability to non-manufacturer defendants and standardized the bases to prove a product defect, products liability has been fully integrated into civil justice jurisprudence. Most significantly, the social objectives of strict products liability articulated by Traynor in *Escola* and Prosser in his *Assault Upon the Citadel* have largely been achieved.

¹²⁹ Model Uniform Product Liability Act, 44 Fed. Reg. 62,714, 62,717, 62,721 (Oct. 31, 1979).

¹²⁴ Hylton, *supra* note 85, at 2469.

¹²⁵ Id.

¹²⁶ Id.

¹²⁷ Brazil v. Janssen Rsch. & Dev. LLC, 196 F. Supp. 3d 1351, 1358 (N.D. Ga. 2016); Seattle-First Nat'l Bank v. Tabert, 542 P.2d 774, 776 (Wash. 1975).

¹²⁸ *Brazil*, 196 F. Supp. 3d at 1359–60; Battersby v. Boyer, 526 S.E.2d 159, 162 (Ga. Ct. App. 1999).

¹³⁰ Hylton, *supra* note 85, at 2470.

[Vol. 26.4

III. SECTION 230: PRIVITY DOCTRINE OF THE INTERNET AGE

LEWIS & CLARK LAW REVIEW

Historians and commentators have characterized the emergence of the internet over the past 30 years as analogous to the Industrial Revolution in terms of its political, social, economic, and cultural impacts.¹³¹ Like the Industrial Revolution in the 19th century, the digital revolution has caused wide scale disruption of social and economic relationships, as new manufacturing technologies and marketing relationships have transformed the nature of work, finance, and commerce. Like the advent of the steam engine in the early 1800s, the emergence of the internet age was initially hailed with euphoria and optimism as the harbinger of a new economic and political era. Just as 19th-century courts sought to remove legal constraints on manufacturers that were the deliverers of new technology, in the late 20th century, courts and legislators sought to liberate online companies from traditional legal obligations that curtailed expansion in the new digital economy.¹³²

A. Origins of Section 230

The Communications Decency Act (CDA) was enacted in 1996 when just 7% of Americans had access to the internet, Netscape was the dominant search engine, Google did not exist, and Facebook's launch was eight years away.¹⁸³ Enacted at the height of optimism over the transformative potential of the internet, CDA sought "to promote the continued development of the Internet and other interactive computer services" and "preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."¹³⁴ However, as the late Chief Judge Katzman observed "[t]he

¹³¹ See Thomas L. Friedman, The World Is Flat: A Brief History of the Twenty-First Century 202–04, 323 (2005); Klaus Schwab, The Fourth Industrial Revolution 11–13 (2016).

¹³² See generally SCHWAB, supra note 131.

¹³³ Farhad Manjoo, *Jurassic Web: The Internet of 1996 Is Almost Unrecognizable Compared* with What We Have Today, SLATE (Feb. 24, 2009, 5:33 PM), https://slate.com/technology/ 2009/02/the-unrecognizable-internet-of-1996.html.

 $^{^{134}}$ 47 U.S.C. § 230(b)(1), (2). Section 230 was enacted in response to *Stratton Oakmont*, *Inc. v. Prodigy Services Co.*, No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), where a New York court held that an online bulletin board could be held strictly liable for third parties' defamatory posts. The court rejected the defendant's argument that it was a mere "distributor" of third-party content, holding that the defendant's screening and editing of posts made it a primary publisher and therefore vicariously liable for defamatory content on its platform. *Id.* at *4–6.

text and legislative history of [§ 230(c)(1)] shout to the rafters Congress's focus on reducing children's access to adult material."¹³⁵ Entitled "Protection for private blocking and screening of offensive material," § 230 reflected a Congressional finding that "it is the policy of the United States to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material."¹³⁶ In furtherance of this policy, § 230(c)—entitled "Protection for 'Good Samaritan' blocking and screening of offensive material"—provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."¹³⁷

In adopting § 230, Congress was also motivated to override a recent decision of a New York trial court in *Stratton Oakmont, Inc. v. Prodigy Services Co.*¹³⁸ In *Stratton*, an internet service provider was held liable for a third party's libelous statements posted on its computer bulletin boards.¹³⁹ Then-representatives Christopher Cox and Ron Wyden proposed an amendment to the draft CDA (the Cox–Wyden Proposal).¹⁴⁰ The Cox–Wyden Proposal sought to address the dilemma *Stratton* created by removing traditional forms of publisher liability for internet service providers that acted in good faith to restrict access to offensive content.¹⁴¹ Under § 230, plaintiffs may hold liable the person who creates or develops unlawful content, but not the interactive computer service provider that merely *enables* such content to be posted online.¹⁴² Section 230 represents congressional optimism that, unfettered by artificial restrictions, the internet would usher in a new era of social and economic progress.

B. Broad Construction of Section 230

Early appellate decisions applied an expansive interpretation of § 230 to confer broad immunity for online platforms. Just as Prosser described the "citadel" of con

¹³⁵ Force v. Facebook, Inc., 934 F.3d 53, 88 (2d Cir. 2019) (Katzman, C.J., dissenting in part) (citing legislative history): *see also* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1163 (9th Cir. 2008) (en banc) (explaining that § 230 was enacted to protect interactive content providers who *restrict* access to objectionable material).

¹³⁶ 47 U.S.C. § 230(b)(4).

¹³⁷ 47 U.S.C. § 230(c)(1).

¹³⁸ Stratton Oakmont, Inc., 1995 WL 323710.

¹³⁹ Id. at *7.

 $^{^{\}rm 140}\,$ 141 CONG. REC. 22,044 (1995) (statements of Rep. Christopher Cox and Rep. Ron Wyden).

 $^{^{141}}$ Id.

¹⁴² Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc., 591 F.3d 250, 254 (4th Cir. 2009) (construing § 230(c)(1)).

tractual privity to protect manufacturers from liability for their injurious products, Professors Danielle Keats Citron and Benjamin Wittes observe that "courts have built a mighty fortress protecting platforms from accountability for unlawful activity

The Fourth Circuit's 1997 decision in Zeran v. America Online, Inc.¹⁴⁴ had a similar impact on the internet revolution that *Winterbottom* had on the Industrial Revolution. Zeran arose out of a series of anonymous posts on America Online, Inc. (AOL) falsely claiming that the plaintiff, Zeran, was selling consumer products with "offensive and tasteless slogans related to the April 19, 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City," and instructing purchasers to call the plaintiff's home number if they wanted to place an order.¹⁴⁵ As a result of this anonymous prank, Zeran was deluged with angry and derogatory messages, including death threats.¹⁴⁶ Zeran made repeated calls to AOL requesting that the derogatory posts be removed and that AOL post a retraction, but was unable to obtain prompt relief.¹⁴⁷

Zeran filed suit alleging that "AOL unreasonably delayed in removing defamatory messages posted by an unidentified third party, refused to post retractions of those messages, and failed to screen for similar postings thereafter."¹⁴⁸ AOL argued that, because the plaintiff's injury arose out of online content posted by third parties, his claim was barred by § 230. The district court dismissed the case on its pleadings, and the Fourth Circuit affirmed.¹⁴⁹

Decided at a time when courts felt the need to explain what the internet is,¹⁵⁰ the Fourth Circuit adopted a triumphalist view of new technology, concluding that "interactive computer services 'have flourished, to the benefit of all Americans.'"¹⁵¹ Selectively quoting from the statute, the court held that § 230 was enacted "to maintain the robust nature of Internet communication [as]... 'a forum for a true

1180

on their systems."143

¹⁴³ Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401, 406 (2017).

¹⁴⁴ Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997).

¹⁴⁵ Id. at 329.

¹⁴⁶ Id.

¹⁴⁷ Id.

¹⁴⁸ Id. at 328.

¹⁴⁹ Id. at 328-30.

¹⁵⁰ See id. at 328 ("'The Internet is an international network of interconnected computers,' currently used by approximately 40 million people worldwide." (quoting Reno v. Am. C.L. Union, 521 U.S. 844, 849 (1997))).

¹⁵¹ Id. at 330 (quoting 47 U.S.C. § 230(a)(4)).

diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.²⁷¹⁵² Armed with the munificent purpose, the Fourth Circuit expanded the plain meaning of § 230 to confer "immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.²¹¹⁵³ Thus, "[a]lthough the text of § 230(c)(1) grants immunity only from 'publisher' or 'speaker' liability, the [court in *Zeran*] held that it eliminates distributor liability too—that is, § 230 confers immunity even when a company distributes content that it *knows* is illegal.²¹⁵⁴ Because Zeran sought to hold AOL liable for defamatory speech initiated by a third party, his claims were barred by § 230.

Zeran also argued that irrespective of the conduct of third parties, AOL possessed actual knowledge of false and defamatory content posted on their platforms.¹⁵⁵ He contended that notwithstanding the third-party origin of the defamatory content, AOL was subject to independent liability for failing to remove the postings once it learned of their falsity and the consequent harassment and death threats.¹⁵⁶

The Fourth Circuit rejected this argument as anachronistic under the "practical implications" of liability in the internet age.¹⁵⁷ Echoing the concerns in *Winterbot-tom* that holding manufacturers liable for their defective products would hobble economic progress, the Fourth Circuit held that imposing a duty on online platforms to remove content that they knew to be harmful would have a chilling effect on free online speech:

If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement—from any party, concerning any message. Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information. Although this might be feasible for the traditional print publisher, the sheer number of

¹⁵² *Id.* (quoting 47 U.S.C. § 230(a)(3)).

¹⁵³ Id.

¹⁵⁴ Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 15 (2020) (Thomas, J., statement respecting denial of certiorari) (citing *Zeran*, 129 F.3d at 331–34).

¹⁵⁵ Zeran, 129 F.3d at 331–32.

¹⁵⁶ Id. at 329, 331.

¹⁵⁷ *Id.* at 333.

postings on interactive computer services would create an impossible burden in the Internet context. . . . Thus, like strict liability, liability upon notice has a chilling effect on the freedom of Internet speech.¹⁵⁸

Following Zeran, "courts have 'consistently... held that § 230 provides a 'robust' immunity, and that all doubts must be resolved in favor of immunity."¹⁵⁹ While § 230 does not define "publisher" or "speaker," state and federal courts have generally held that those terms should also be "construed broadly in favor of immunity."¹⁶⁰ Keats Citron and Wittes observe that these holdings have "produced an immunity from liability that is far more sweeping than anything the law's words, context, and history support."¹⁶¹

With this broad construction of § 230, internet providers "have been protected from liability even though they republished content knowing it might violate the law, encouraged users to post illegal content, [and] changed their design and policies for the purpose of enabling illegal activity."¹⁶² One of the most infamous examples is *Doe v. Backpage.com, LLC*,¹⁶³ which involved a lawsuit by three women who, beginning at age 15, were sex trafficked through advertisements posted on the "Adult Entertainment" section of the Backpage website. Two of the child victims, who were each raped over 900 times, alleged that "Backpage's rules and processes governing the content of advertisements are designed to encourage child sex trafficking."¹⁶⁴ These advertisements included photographs of the plaintiffs and coded terminology such as "brly legal" or "high schl" meant to refer to underage girls.¹⁶⁵ Backpage argued that, because the plaintiffs' claims arose from its publication of the sex traffickers' third-party content, the plaintiffs were barred by § 230, and the First Circuit

¹⁵⁸ Id.

¹⁵⁹ Internet Brands, Inc. v. Jape, 760 S.E.2d 1, 3 (Ga. Ct. App. 2014) (quoting Holomaxx Techs. Corp. v. Microsoft Corp., No. 10-cv-04924, 2011 WL 3740813, at *2 (N.D. Cal. 2011)).

¹⁶⁰ Force v. Facebook, Inc., 934 F.3d 53, 64 (2d Cir. 2019); *see, e.g.*, Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc., 591 F.3d 250, 254 (4th Cir. 2009) ("[C]ourts have generally accorded § 230 immunity a broad scope."); Universal Comme'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 419 (1st Cir. 2007) ("Section 230 immunity should be broadly construed."); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003) ("[R]eviewing courts have treated § 230(c) immunity as quite robust.").

¹⁶¹ Keats Citron & Wittes, *supra* note 143, at 408.

¹⁶² Id.

¹⁶³ Doe v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016).

¹⁶⁴ Id. at 16-17.

¹⁶⁵ Id.

agreed.¹⁶⁶ In language reminiscent of Winterbottom, the court reasoned that "websites that display third-party content may have an infinite number of users generating an enormous amount of potentially harmful content, and holding website operators liable for that content 'would have an obvious chilling effect' in light of the difficulty of screening posts for potential issues."167 Because the plaintiffs' claims related to the structure and operation of Backpage's website, they sought to hold Backpage liable for "choices about what content can appear on the website and in what form," which the court held to be "editorial choices that fall within the purview of traditional publisher functions."168 In reaching this holding, the First Circuit adopted the Fifth Circuit's analysis in Doe v. MySpace, Inc.,¹⁶⁹ where a minor was sexually assaulted by a predator she met through the defendant's website. The plaintiff in *MySpace* argued that the website operator "fail[ed] to implement basic safety measures to protect minors," but the Fifth Circuit rejected the plaintiff's claims on the basis that the claims were "merely another way of claiming that [the website operator] was liable for publishing the communications and they speak to [the website operator's] role as a publisher of online third-party-generated content."¹⁷⁰

C. Growing Dissent

Public outcry over the *Backpage* and *MySpace* decisions led to the introduction of the Stop Enabling Sex Traffickers Act¹⁷¹ and the Allow States and Victims to Fight Online Sex Trafficking Act of 2018,¹⁷² which eliminated § 230 as a defense for websites that knowingly facilitate sex trafficking.¹⁷³ The legislation, passed with wide bipartisan support and signed into law in April 2018,¹⁷⁴ provides that § 230 should not be "construed to impair or limit" victims of commercial sex acts from bringing civil actions against online platforms.¹⁷⁵ However, this amendment did not

¹⁶⁶ *Id.* at 20–22.

¹⁶⁷ Id. at 19 (quoting Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997)).

¹⁶⁸ *Id.* at 21.

¹⁶⁹ Id. (construing Doe v. MySpace, Inc., 528 F.3d 413, 418–20 (5th Cir. 2008)).

¹⁷⁰ MySpace, Inc., 528 F.3d at 419-20.

¹⁷¹ S. 1693, 115th Cong. § 2 (2018) (enacted); S. REP. NO. 115-199, at 2 (2018) (citing Doe v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016)).

¹⁷² Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, 132 Stat. 1253 (2018).

¹⁷³ § 2, 132 Stat. at 1253; S. REP. NO. 115-199, at 2.

¹⁷⁴ See 164 CONG. REC. S1290, 1291 (2018).

^{175 47} U.S.C. § 230(e)(5).

quell the growing recognition among leading jurists,¹⁷⁶ legal scholars,¹⁷⁷ public commentators,¹⁷⁸ and government officials¹⁷⁹ that the broad interpretation of § 230 accorded by courts contravenes its actual legislative intent and is contrary to public policy.

Force v. Facebook, Inc. arose out of attacks against five American citizens in Israel by the Hamas terrorist organization.¹⁸⁰ The plaintiffs alleged that Facebook's algorithms provided Hamas with a forum to promote terrorism and recruit followers.¹⁸¹ Specifically, the plaintiffs claimed that the algorithms that suggested content to users, performed "matchmaking" with other users, and provided targeted "newsfeed" of third-party content most likely to interest users, made Facebook, Inc. a non-publisher under § 230.¹⁸² A majority of the Second Circuit disagreed, holding that "we find no basis . . . for concluding that an interactive computer service is not the 'publisher' of third-party information when it uses tools such as algorithms that are designed to match that information with a consumer's interests."¹⁸³ Chief Judge Katzmann agreed that § 230 protected Facebook, Inc. from liability for allowing Hamas content to be posted on its platform, but dissented from the majority's holding that Facebook's friend- and content-suggestion algorithms constituted protected publishing activity under § 230.¹⁸⁴ Katzmann argued that it "strains the English language to say that in targeting and recommending [content] to users . . . Facebook is

¹⁷⁶ See, e.g., 164 CONG. REC. \$1849, 1860; Danielle Keats Citron & Benjamin Wittes, *The Problem Isn't Just Backpage: Revising Section 230 Immunity*, 2 GEO. L. TECH. REV. 453, 461 (2018) (discussing Chief Judge Frank Easterbrook's majority opinion in *Chi. Laws. Comm. for C.R. v. Craigslist*, 519 F.3d 666 (7th Cir. 2008)).

¹⁷⁷ See, e.g., Keats Citron & Wittes, supra note 176, at 458–59; Daniela C. Manzi, Managing the Misinformation Marketplace: The First Amendment and the Fight Against Fake News, 87 FORDHAM L. REV. 2623, 2642–43 (2019). But see Jeff Kosseff, Defending Section 230: The Value of Intermediary Immunity, 15 J. TECH. L. & POL'Y 123, 145–48 (2010).

¹⁷⁸ See, e.g., Mike Wacker, Opinion, Repeal Section 230 for Child Porn, NEWSWEEK (Sept. 6, 2022, 6:30 AM), https://www.newsweek.com/repeal-section-230-child-porn-opinion-1739141; Kalev Leetaru, A Call to Amend Section 230 for Social Media Transparency, DAILY WIRE (Oct. 16, 2021), https://www.dailywire.com/news/a-call-to-amend-section-230-for-social-media-transparency; Nate Hochman, Conservatives Should Support Section 230 Reform, NAT'L REV. (Oct. 16, 2021, 6:30 AM), https://www.nationalreview.com/2021/10/conservatives-should-support-section-230-reform/; Abbey Stemler, Opinion, What Is Section 230 and What Lies Ahead for Social-Media Reform?, SEATTLE TIMES (Aug. 3, 2021, 2:30 AM), https://www.seattletimes.com/opinion/what-is-section-230-and-what-lies-ahead-for-social-media-reform/.

¹⁷⁹ See, e.g., Rebecca Kern, White House Renews Call to Remove' Section 230 Liability Shield, POLITICO, https://www.politico.com/news/2022/09/08/white-house-renews-call-to-removesection-230-liability-shield-00055771 (Sept. 9, 2022, 12:39 PM).

¹⁸⁰ Force v. Facebook, Inc., 934 F.3d 53, 57 (2d Cir. 2019).

¹⁸¹ Id. at 59, 65.

¹⁸² *Id.* at 65.

¹⁸³ *Id.* at 66.

¹⁸⁴ *Id.* at 76–77, 82–83 (Katzmann, C.J., concurring in part and dissenting in part).

acting as 'the *publisher* of . . . information provided by another information content provider."¹⁸⁵ The recommendation of a defendant "conveyed a message from the defendant itself, and thus was not merely publishing content treated by another party."¹⁸⁶

Katzmann undertook an extensive analysis of § 230's legislative history, arguing that there is no basis for concluding that algorithmic content recommendations designed to match content with users constituted the publishing activity that Congress sought to protect.¹⁸⁷ Katzmann reasoned:

It would be one thing if congressional intent compelled us to adopt the majority's reading. It does not. Instead, we today extend a provision that was designed to encourage computer service providers to shield minors from obscene material so that it now immunizes those same providers for allegedly connecting terrorists to one another. Neither the impetus for nor the text of \$230(c)(1)\$ requires such a result. When a plaintiff brings a claim that is based not on the content of the information shown but rather on the connections Facebook's algorithms make between individuals, the CDA does not and should not bar relief.¹⁸⁸

While acknowledging that posting terrorist propaganda online is protected activity, Katzmann observed that:

[P]laintiffs' claims do not seek to punish Facebook for the content others post, for deciding whether to publish third parties' content, or for editing (or failing to edit) others' content before publishing it. . . . Instead, they would hold Facebook liable for its affirmative role in bringing terrorists together.¹⁸⁹

Katzmann's partial dissent was favorably invoked by Justice Clarence Thomas in his statement accompanying the U.S. Supreme Court's denial of certiorari in *Malwarebytes, Inc. v. Enigma Software Group USA, LLC.*¹⁹⁰ In *Malwarebytes,* the Ninth Circuit declined to apply § 230 to a dispute where "defendant, Malwarebytes Inc., [had] configured its software to block users from accessing [plaintiff] Enigma's software in order to divert Enigma's customers."¹⁹¹ Thomas agreed with the Supreme Court's decision not to take up the case, but wrote to urge that "in an appro-

¹⁸⁵ Id. at 76-77 (quoting 47 U.S.C. § 230(c)(1)).

¹⁸⁶ Petition for Writ of Certiorari at 14, Gonzalez v. Google LLC, No. 21-1333 (U.S. Apr. 4, 2022), 2022 WL 1050223, at *14.

¹⁸⁷ Force, 934 F.3d at 77-80.

¹⁸⁸ *Id.* at 77.

¹⁸⁹ Id.

¹⁹⁰ Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 17 (2020) (Thomas, J., statement respecting denial of certiorari).

¹⁹¹ Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1044, 1051 (9th Cir. 2019).

priate case, we should consider whether the text of this increasingly important statute aligns with the current state of immunity enjoyed by Internet platforms."¹⁹² Reciting the legislative history of § 230, Thomas castigated lower courts for relying "on policy and purpose arguments to grant sweeping protection to Internet platforms."193 He pointed out that, while § 230 only references publishers and speakers, courts have extended immunity to distributors as well.¹⁹⁴ Thomas further argued that courts have improperly extended § 230 to immunize internet platforms for their own content and conduct.¹⁹⁵ Referencing the Backpage and Force decisions, Thomas castigated lower courts for extending § 230 publisher immunity to bar claims alleging that platforms promoted terrorism and facilitated sex trafficking of minors.¹⁹⁶ He explained:

A common thread through all these cases is that the plaintiffs were not necessarily trying to hold the defendants liable 'as the publisher or speaker' of thirdparty content. Nor did their claims seek to hold defendants liable for removing content in good faith. Their claims rested instead on alleged product design flaws-that is, the defendant's own misconduct.¹⁹⁷

Thomas acknowledged that Malwarebytes was not the vehicle for "[p]aring back the sweeping immunity courts have read into § 230," but urged that "in an appropriate case, it behooves us to do so."198

D. Gonzalez v. Google: Pathway for Expanding Products Liability Exception to Section 230 Immunity

In Gonzalez v. Google LLC,¹⁹⁹ the Ninth Circuit considered whether § 230 barred claims against Google for aiding and abetting ISIS terrorist attacks by recommending ISIS content to users. The plaintiffs alleged that Google used computer algorithms to match and suggest terrorist videos to users based on their viewing history, that these recommendations "were critical to the growth and activity of ISIS," and "that Google officials were well aware that the company's services were

¹⁹² Malwarebytes, 141 S. Ct. at 14 (Thomas, J., statement respecting denial of certiorari). ¹⁹³ Id. at 15.

¹⁹⁴ Id. (citing Zeran v. Am. Online, Inc., 129 F.3d 327, 331–34 (4th Cir. 1997)).

¹⁹⁵ *Id.* at 16.

¹⁹⁶ Id. at 17.

¹⁹⁷ Id. at 18 (citing 47 U.S.C. § 230(c)(1)–(2)).

¹⁹⁸ Id.

¹⁹⁹ Gonzalez v. Google LLC, 2 F.4th 871 (9th Cir. 2021). The Ninth Circuit opinion addressed three appeals concerning the liability of Google, Twitter, and Facebook in connection with acts of terrorism in Paris, Istanbul, and San Bernardino. The plaintiffs in the Gonzalez appeal were the family members of an American student who was killed at a Paris café in 2015 in an attack perpetrated by the Islamic States of Iraq (ISIS). Id. at 879-81.

assisting ISIS."²⁰⁰ However, the plaintiffs did not allege that Google had targeted ISIS content specifically or designed its website to support terroristic videos or ideals.²⁰¹

Writing for the court, Judge Morgan Christen followed the Second Circuit's analysis in *Force*, holding that Google's algorithmic recommendations were protected by § 230 because "Google provided a neutral platform that did not specify or prompt the type of content to be submitted, nor determine particular types of content its algorithms would promote."²⁰² The court explained that:

[A] user's voluntary actions inform Google about that user's preferences for the types of videos and advertisements the user would like to see. . . . Google matches what it knows about users based on their historical actions and sends third-party content to users that Google anticipates they will prefer. This system is certainly more sophisticated than a traditional search engine, which requires users to type in textual queries, but the core principle is the same: Google's algorithms select the particular content provided to a user based on that user's inputs.²⁰⁸

Judge Marsha Berzon agreed that the court's holding was compelled by Ninth Circuit precedent but wrote separately to "join the growing chorus of voices calling for a more limited reading of the scope of section 230 immunity."²⁰⁴ Adopting the reasoning "compellingly given" in Katzmann's partial dissent in *Force*, Berzon explained that:

[I]f not bound by Circuit precedent I would hold that the term 'publisher' under section 230 reaches only traditional activities of publication and distribution—such as deciding whether to publish, withdraw, or alter content and does not include activities that promote or recommend content or connect content users to each other.²⁰⁵

She urged the Ninth Circuit to "reconsider our precedent *en banc* to the extent that it holds that § 230 extends to the use of machine-learning algorithms to recommend content and connections to users."²⁰⁶

²⁰⁰ *Id.* at 882; Petition for Writ of Certiorari, *supra* note 186, at 10–12, 2022 WL 1050223, at *10–12.

²⁰¹ Gonzalez, 2 F.4th at 895.

²⁰² *Id.* The court clarified that, "we do not hold that 'machine-learning algorithms can *never* produce content within the meaning of Section 230.' We only reiterate that a website's use of content-neutral algorithms, without more, does not expose it to liability for content posted by a third-party." *Id.* at 896 (quoting *id.* at 913 (Berzon, J., concurring)).

²⁰³ Id. at 895.

²⁰⁴ Id. at 913 (Berzon, J., concurring).

²⁰⁵ *Id.* (citing with approval Force v. Facebook, Inc., 934 F.3d 53 (2d Cir. 2019) (Katzmann, C.J., concurring in part and dissenting in part)).

²⁰⁶ Id. at 917.

291

Judge Ronald Gould dissented in part on the ground that § 230 was not intended to immunize "companies providing interactive computer services from liability for serious harms knowingly caused by their conduct."²⁰⁷ Gould agreed with Katzmann's "cogent and well-reasoned opinion" in *Force*, which he attached to his partial dissent.²⁰⁸ However, he went further in positing that § 230 does not "wholly immunize[] a social media company's role as a channel of communication for terrorists in their recruiting campaigns and as an intensifier of the violent and hatredfilled messages they convey."²⁰⁹ Rejecting the hair-splitting distinctions used by prior courts in finding algorithms to be content-neutral tools, Gould argued that where a website "(1) knowingly amplifies a message designed to recruit individuals for a criminal purpose, and (2) the dissemination of that message ... give[s] rise to a probability of grave harm, then the tools can no longer be considered 'neutral."²¹⁰

Moving beyond narrow questions of statutory construction, Gould addressed the larger public policy issues implicated by the court's interpretation of § 230. Echoing Traynor, he acknowledged that "at the dawn of the Internet era," it was appropriate to "give protection to Internet companies to facilitate growth. But it is quite another thing to provide broad immunity at a time such as now when such companies are remarkably large."²¹¹ While agreeing it would be "preferable if the social media companies monitored their own activities sufficiently to protect the public," Gould suggested that it was "not realistic to anticipate that social media companies will self-police adequately in the face of their incentives to maximize profits by maximizing advertising revenues."²¹² Noting that "[s]ociety for centuries has known that it is folly to ask the fox to guard the henhouse," he argued that it makes no sense to entrust the responsibility of protecting the public "to the selfinterested proclamations of CEOs or other employees of the various social media companies."²¹³

Looking at the historical foundations of tort law, Gould observed that tort law emerged "to provide a doctrinal basis for remedy in the case of injuries from harmful and unreasonable conduct."²¹⁴ Applying this principle to the carte blanche immunity that social media companies enjoy under § 230, he urged that they "be held to some reasonable standard of conduct when they have failed to regulate their own

²¹³ Id.

²⁰⁷ Id. at 920 (Gould, J., concurring part and dissenting in part).

²⁰⁸ *Id.* at 920, 938 attach. A (citing with approval *Force*, 934 F.3d 53 (Katzmann, C.J., concurring in part and dissenting in part)).

²⁰⁹ Id. at 920-21.

²¹⁰ Id. at 923.

²¹¹ Id. at 936; see Traynor, supra note 52.

²¹² Gonzalez, 2 F.4th at 936 (Gould, J., concurring in part and dissenting in part).

 $^{^{214}}$ Id. at 937 (citing Frederick Pollock, The Law of Torts: A Treatise on the Principles of Obligations Arising from Civil Wrongs in the Common Law 19–20 (4th ed. 1895)).

actions in the interests of the public.²¹⁵ Applying traditional products liability theory, Gould argued that "when social media companies in their platforms use systems or procedures that are unreasonably dangerous to the public... then there should be a federal common law claim available against them."²¹⁶ Gould reasoned:

[M]anufacturers are responsible in tort if they make unreasonably dangerous products that cause individual or social harm. Section 402A states: "One who sells any product in a defective condition unreasonably dangerous to the user or consumer or to his property is subject to liability for physical harm thereby caused" to the user or a third party. Here and similarly, social media companies should be viewed as making and "selling" their social media products through the device of forced advertising under the eyes of users. Viewed in this light, they should be tested under a federal tort principle with a standard similar to and adapted from this *Restatement* language under a federal common law development. If social media companies use "neutral" algorithms that cause unreasonably dangerous consequences, under proper standards of law with limiting jury instructions, they might be held responsible.²¹⁷

Nevertheless, recognizing the difficulty of these issues, Gould urged that "it would be desirable for the Supreme Court to take up the subject of Section 230 immunity."²¹⁸

The plaintiffs petitioned for rehearing en banc. Gould and Berzon voted to grant the petition, and Christen voted to deny it.²¹⁹ The Ninth Circuit held a vote on whether to rehear *Gonzalez* en banc, but the decision failed to receive a majority of the votes of the non-recused active judges.²²⁰ Gould dissented from the order, incorporating by reference his partial dissent in *Gonzalez*.²²¹

The *Gonzalez* plaintiffs petitioned for certiorari on the question of whether § 230 "immunize[s] interactive computer services when they make targeted recommendations of information provided by another information content provider, or only limit[s] the liability of interactive computer services when they engage in traditional editorial functions (such as decided whether to display or withdraw) with regard to such information."²²² The plaintiff–petitioners focused on Katzmann's "exceptionally detailed and scholarly" partial dissent in *Force*, and Gould's partial dissent and Berzon's concurrence in *Gonzalez*, observing that "[e]very member of

²¹⁵ Id. at 937-38.

²¹⁶ Id. at 938.

 $^{^{217}}$ $\,$ Id. at 938 (citing Restatement (Second) of Torts § 402A (Am. L. Inst. 1965)).

²¹⁸ Id. at 937.

²¹⁹ Gonzalez v. Google LLC, 21 F.4th 665 (9th Cir. 2022) (mem.).

²²⁰ Id.

²²¹ Id. (incorporating by reference Gonzalez, 2 F.4th at 918–52 (Gould, J., concurring in part and dissenting in part)).

²²² Petition for Writ of Certiorari, *supra* note 186, at i, 2022 WL 1050223, at *i.

the panel below expressed misgivings about the increasing breadth with which section 230 has been construed by the lower courts."²²³ Google opposed the petition for certiorari arguing, "no circuit suggests, much less holds, that section 230 exempts 'targeted recommendations' from coverage. . . . The continued uniformity among the circuits over both the question presented and broader questions about section 230 are reason enough to deny review."²²⁴ Google observed that the Court "has already denied numerous section 230 petitions, including two recent petitions raising virtually identical questions,"²²⁵ and that the uniform conclusion among the federal circuits that § 230 applies to neutral algorithms displaying recommended content is manifestly correct.²²⁶ Google urged the Court to "not lightly adopt a reading of section 230 that would threaten the basic organizational decisions of the modern internet."²²⁷ Undaunted by this prospect, the U.S. Supreme Court granted certiorari on October 3, 2022.²²⁸

IV. APPLICATION OF PRODUCTS LIABILITY THEORY TO CHALLENGE UNREASONABLY DANGEROUS SOCIAL MEDIA PLATFORMS

Traynor's characterization of products liability law as ameliorating the rampages of the Industrial Revolution²²⁹ is equally applicable to the current transition from an industrial to a post-industrial society. As Gould observed in his partial dissent in *Gonzalez*, strict products liability provides a viable legal vehicle to counter the harsh social costs of the computer revolution and to reverse the growing social harms arising from virtually unregulated social media use. Social media platforms operate on complex computer algorithms invisible and incomprehensible to ordinary consumers. Traynor's public policy imperative—that liability be affixed on the party in the best position to reduce the hazards to life and health posed by dangerous products—is particularly applicable considering the wide disparity of information between social media platforms and their users.²³⁰ Based on their design, operation, and monitoring algorithms that fuel consumers' use of their products, social media

²²³ Id. at 4-5, 16, 20, 2022 WL 1050223, at *4-5, *16, *20.

²²⁴ Brief in Opposition at 13–14, Gonzalez v. Google LLC, No. 21-1333 (U.S. July 5, 2022), 2022 WL 2533118, at *13–14.

²²⁵ Id. at 9 n.1, 14, 2022 WL 2533118, at *9 n.1, *14.

²²⁶ Id. at 20–22, 2022 WL 2533118, at *20–22.

²²⁷ Id. at 22, 2022 WL 2533118, at *22.

²²⁸ Gonzalez v. Google LLC, No. 21-1333, 2022 WL 4651229 (U.S. Oct. 3, 2022).

²²⁹ Traynor, *supra* note 52, at 364.

²³⁰ See, e.g., Escola v. Coca Cola Bottling Co., 150 P.2d 436, 440 (Cal. 1944) (noting that the defendant had "exclusive control over both the charging and inspection of the bottles").

companies can anticipate many hazards and guard against the recurrence of others while the public cannot. $^{\rm 231}$

The mental health epidemic currently ravaging American youth demonstrates that those suffering injury from defective social media products are unprepared to meet its consequences.²⁹² The overwhelming cost of injury can be insured by social media product manufacturers "as a cost of doing business."²³³ "Against such a risk, there should be general and constant protection, and the manufacturer is best situated to afford such protection."²³⁴

Strict liability to social media product manufacturers serves not only the interest of public policy, but also the interest of economic efficiency. Scholars generally agree that, from a legal and economic standpoint, an efficient and effective products liability regime accomplishes two goals: "First, it would encourage parties to prevent all preventable accidents (the 'deterrence' goal). Second, it would efficiently allocate the risk of prevented accident costs (the 'insurance' goal)."²³⁵ Professor Daniel Jones explains that, "From an economic point of view, negligence law attempts to shift the burden of the negative externality caused by the tortfeasor's actions from the victim to the tortfeasor."²³⁶ He further observes:

[T]here are two general types of costs: the costs the tortfeasor can recognize (internal/precaution costs) and the costs imposed on other people as a result of the tortfeasor's actions (external/accident costs). The "external costs" are [those] borne by the plaintiff and any other member of society affected by the tortfeasor's actions. "Internal costs" are primarily the costs associated with the level of precaution incorporated by the tortfeasor.²⁵⁷

As Hylton explains:

Under strict products liability, the risk cost is internalized to the producer, so that the unit profit of selling the risky model is reduced by the expected liability....

Thus, under strict liability, the producer will choose the risky design if the incremental utility is greater than the incremental risk. It follows that strict products liability optimally regulates design choice.²⁸⁸

²³¹ See id. at 440-41 (Traynor, J., concurring).

²³² See supra notes 26-41 and accompanying text.

²³³ Escola, 150 P.2d at 438 (Traynor, J., concurring).

²³⁴ Id. at 441.

²³⁵ Jon D. Hanson & Kyle D. Logue, *The First-Party Insurance Externality: An Economic Justification for Enterprise Liability*, 76 CORNELL L. REV. 129, 135 (1990).

²³⁶ Daniel Jones, An Economic Analysis of Montana Products Liability, 71 MONT. L. REV. 157, 158 (2010).

²³⁷ Id. at 159.

²³⁸ Hylton, *supra* note 85, at 2478 (emphasis omitted).

Similarly, Jones notes that "[a]s long as the manufacturer is forced to internalize the external costs its actions impose upon society, the manufacturer will have an incentive to minimize both the expected accident costs and its internal precaution costs."²²⁹

The economic imperative to internalize safety costs is particularly acute where a wide disparity of information exists between the manufacturer and consumer. A decade before the advent of the internet, Posner and Professor William Landes observed that "[t]he growth in the technical complexity of products . . . has been accompanied by a decline in the technical knowledge of consumers as consumers."²⁴⁰ Posner and Landes asserted that as the complexity of products increases, the cost to the consumer of obtaining relevant information about the product rises. And as the cost of acquiring useful information about the product goes up, consumers' ability to rely on their own due care to protect themselves from design defects or inherent hazards is reduced.²⁴¹

Consumers that lack sufficient knowledge about a product's dangers are unable to optimally factor the risk of harm into their market activity.²⁴² Indeed, Posner noted that "strict liability in effect impounds information about product hazards into the price of the product, resulting in a substitution away from hazardous products by consumers who may be completely unaware of the hazards."²⁴³ The positive economic theory of strict products liability embraced by Landes, Posner, Hylton, and Jones maps precisely onto the normative case for applying strict liability to social media platforms. The reason is simple: the complexity of social media products and the inherent hazards in their design create a high transactional cost for consumers to obtain the information they would need to use the product safely.

²³⁹ Jones, *supra* note 236, at 163.

²⁴⁰ William M. Landes & Richard A. Posner, *A Positive Economic Analysis of Products Liability*, 14 J. LEGAL STUD. 535, 548 (1985).

²⁴¹ Id. at 547–51.

 $^{^{242}\,}$ Id. at 550. Hylton explained the merits of products liability principles to the consumer as follows:

In the absence of products liability there is likely to be overconsumption of risky products and an excessive tendency on the part of producers to choose designs with hidden risks.... If a new product design appears on the market, and its incremental risks are obviously greater than its incremental utility, relative to some safer alternative available, consumers will tend not to purchase the new product.... In contrast, consumers do not have sufficient information on the risk characteristics of complicated products to be able to take the precise risks into account in purchasing decisions. It follows that the products on the market that have risks in excess of benefits to consumers (relative to safer available alternatives) are likely to be those for which the risks are unobservable or in some sense likely to be passed over by the consumer until it is too late.

Hylton, supra note 85, at 2501.

²⁴³ POSNER, *supra* note 91, § 6.6, at 166.

The significant technical complexity of social media platforms effectively eliminates consumers' capacity to avoid the design hazards inherent to the product. For products with such expensive information asymmetry, the most efficient outcome is achieved when strict liability attaches to the party with the lowest-cost access to relevant information about the product's harmful attributes. In most cases, that party is the manufacturer; in this case, it is the social media platform. For example, one of the fundamental characteristics of social media platforms is an artificial intelligence (AI) recommendation function that determines what content consumers will be shown next. These algorithmic engines "learn" consumer preferences and deploy that information to keep users engaged, and they operate at the core of social media platform revenue streams.²⁴⁴

The basic economic model of a social media platform is simple: advertisers purchase space on the platform, and the algorithms work behind the scenes to connect consumers with advertisements specifically tailored to their interests. And because advertising revenue is generated by user engagement (views, clicks, etc.), social media platforms and their content-recommendation algorithms are designed to keep consumers coming back for more—described by one developer "as if they're taking behavioral cocaine and just sprinkling it all over your interface . . . to make it maximally addicting."²⁴⁵ However, because the nature of the product's inherent risk is not readily apparent to consumers—the harmful element of social media platforms, i.e., the exploitation of human psychology to generate revenue, is part of their design—there is no reason to assume that users have accepted a known risk.²⁴⁶

This is particularly true because social media platforms are readily available to children, and the platforms are not subject to any regulatory safeguards in place to prevent abuse. In fact, early regulation of the internet created liability shields for these companies that allow them to avoid accountability for harms perpetrated by third parties on their platforms. Today, social media companies are permitted to not just host but, in fact, *guide* minor users toward grotesquely harmful content—including predatory communications, online bullying, and child sex trafficking—under § 230's expansive immunity.

Finally, while Congress and regulatory agencies are considering legislation to make social media platforms safer for users, there is reason to doubt that these efforts

²⁴⁴ See Pasquale Lops, Marco de Gemmis & Giovanni Semeraro, *Content-Based Recommender Systems: State of the Art and Trends, in* RECOMMENDER SYSTEMS HANDBOOK 73, 79–80 (Francesco Ricci, Lior Rokach, Bracha Shapira & Paul B. Kantor eds., 2010).

²⁴⁵ Hilary Andersson, *Social Media Apps Are 'Deliberately' Addictive to Users*, BBC (July 4, 2018), https://www.bbc.com/news/technology-44640959 (quoting Aza Raskin, inventor of the infinite scroll feature).

²⁴⁶ Allison Zakon, Optimized for Addiction: Extending Product Liability Concepts to Defectively Designed Social Media Algorithms and Overcoming the Communications Decency Act, 2020 WIS. L. REV. 1107, 1129 (2020).

will be sufficient in the absence of civil justice remedies to curb the hazards of such products. Hylton explains:

Given the low likelihood that regulatory agencies could manage the scale of activity reviewed under products liability law, or could craft rules that target with precision the product risks that should be controlled, products liability law performs a regulatory function that could not be supplanted by regulators.²⁴⁷

While regulation will furnish an important role in curbing the harms, particularly to children, from social media use, only a regime of products liability can fully incentivize optimal safety in platforms. By definition, regulations are promulgated based on government regulators' current knowledge of regarding product hazards and safer alternatives.²⁴⁸ In contrast, under traditional products liability, manufacturers are held to the knowledge and skill of an expert, meaning that "at a minimum he must keep abreast of scientific knowledge, discoveries, and advances and is presumed to know what is imparted thereby. But even more importantly, a manufacturer has a duty to test and inspect his product."²⁴⁹ Thus, a products liability regime that places the burden of safety on the manufacturer will always provide greater protection to the consumer than regulation alone.

V. ASSAULTING SECTION 230 THROUGH PRODUCTS LIABILITY

The broad construction of § 230 has generally focused on internet platforms as services, with relatively little emphasis on their status as product manufacturers. Although social media platforms are economically and technologically complex, the case for their treatment as a product, rather than a service, is a strong one.

A. Social Media Platforms Are Products

1194

Products liability case law has steadily progressed toward recognizing intangible goods, such as computer software, as products. A district court in California summarized this development: "Generally, courts have found that mass-produced, standardized, or generally available software, even with modifications and ancillary

²⁴⁷ Hylton, *supra* note 85, at 2503.

²⁴⁸ Tort Liability Versus Insurance and Regulation, JUSTIA, https://www.justia.com/injury/ docs/us-tort-liability-primer/tort-liability-versus-insurance-and-regulation/ (Oct. 2022). ("Whereas tort claims arise after specific injuries occur, efficient regulation requires before-the-fact information about risks of injury, types of precaution, and the costs and benefits associated with particular regulatory standards."). See generally Susan Rose-Ackerman, Regulation and the Law of Torts, 8 AM. ECON. REV. 54 (1991).

²⁴⁹ Borel v. Fibreboard Paper Prods. Corp., 493 F.2d 1076, 1089–90 (5th Cir. 1973).

services included in the agreement, is a good that is covered by the UCC."²⁵⁰ Indeed, social media companies explicitly describe their platforms as "products" that are both standardized and generally available.²⁵¹

Recommendation algorithms are components of software that operate at the core of social media platforms.²⁵² Personalization of the platform to each consumer's preferences is a function of the product's algorithmic learning and data collection. Since these traits categorize software as a good under commercial law, it would be "disconsonant to insist on a different standard" in tort.²⁵³

Moreover, social media companies affirmatively present their platforms as products. Facebook, Inc. itself proclaimed that "[t]o build a *product* that connects people across continents and cultures, we need to make sure everyone can afford it."²⁵⁴ This feature of social media leads to one possible economic distinction: most platforms are not purchased by consumers in the traditional sense. Facebook, for example, is free to use and requires only that users sign a lengthy set of terms and conditions that relinquishes, inter alia, any right they might have had to the ownership and privacy of information generated by their use of the platform.²⁵⁵ This exchange provides consideration for the agreement, yet social media user agreements, in fact, flip the script. By using the product, consumers generate information that the social media platform can either sell to advertisers directly, use to target consumers with highly personalized advertisements, or both.

B. Judicial Application of Products Liability to Social Media Platforms

Several courts have recognized social media platforms as "products" for the purposes of establishing liability for defective design elements. The first case to distinguish products liability claims from § 230 immunity was *Maynard v. Snapchat Inc.*, a decision by the Georgia Court of Appeals.²⁵⁶ *Maynard* arose out of a high-

²⁵⁰ Simulados Software, Ltd. v. Photon Infotech Priv., Ltd., 40 F. Supp. 3d 1191, 1199 (N.D. Cal. 2014).

²⁵¹ Rob Goldman, *Hard Questions: What Information Do Facebook Advertisers Know About Me*?, META (Apr. 23, 2018), https://about.fb.com/news/2018/04/data-and-advertising/.

²⁵² Zakon, *supra* note 246, at 1111–12.

²⁵³ Id. at 1124.

²⁵⁴ Goldman, *supra* note 251 (emphasis added).

²⁵⁵ *Terms of Service*, FACEBOOK, META, https://www.facebook.com/terms.php (last visited Nov. 4, 2022) ("Specifically, when you share, post, or upload content that is covered by intellectual property rights on or in connection with our Products, you grant us a non-exclusive, transferable, sub-licensable, royalty-free, and worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content (consistent with your privacy and application settings.").

²⁵⁶ Maynard v. Snapchat, Inc., 816 S.E.2d 77 (Ga. Ct. App. 2018).

speed auto collision in which the driver was using Snapchat at the time of the accident.²⁵⁷ The court described the platform as follows:

Snapchat is an application made for mobile devices that allows users to take temporary photos and videos, also known as "Snaps," and share them with friends. Snapchat creates "filters" that allow users to include captions, drawings, and graphic overlays on a user's photos or videos. One of these filters is a speedometer that shows the speed at which a user is moving and allows for that speed to be superimposed to a Snap before sending it out over the application.²⁵⁸

The plaintiffs claimed that the driver was using Snapchat while driving more than 100 mph at the time of the crash; as a result, the plaintiffs sued Snapchat, Inc., alleging that its product "encourages" dangerous speeding, and thus contributed to the crash.²⁵⁹

The trial court dismissed the action, holding that Snapchat, Inc. was immune to suit under § 230 because the company was merely the publisher, rather than the creator, of third-party content.²⁶⁰ The court of appeals acknowledged the "robust immunity" conferred on social media platforms by § 230.²⁶¹ Nevertheless, the court reasoned that because the plaintiff's claim arose from the design of the product, rather than from third-party content, § 230 did not bar the claim:

[T]here was no third party content uploaded to Snapchat at the time of the accident and the Maynards do not seek to hold Snapchat liable for publishing a Snap by a third-party that utilized the Speed Filter. Rather, the Maynards seek to hold Snapchat liable for its own conduct, principally for the creation of the Speed Filter and its failure to warn users that the Speed Filter could encourage speeding and unsafe driving practices. Accordingly, we hold that CDA immunity does not apply because there was no third-party user content published.²⁰²

The Ninth Circuit's recent decision in *Lemmon v. Snap, Inc.*²⁶³ rejected the expansive interpretation of § 230 on similar grounds. *Lemmon* arose from a fatal car accident involving two 17-year-olds and a 20-year-old who drove off the road while driving in excess of 100 mph. Shortly before the fatal accident, one of the boys was using the Speed Filter on his Snapchat.²⁶⁴ The court explained that "[t]o keep its

²⁵⁷ Id. at 78–79.

²⁵⁸ *Id.* at 79.

²⁵⁹ Id.

²⁶⁰ Id.

²⁶¹ Id. at 80 (quoting Internet Brands, Inc. v. Jape, 760 S.E.2d 1, 3 (Ga. Ct. App. 2014)).

²⁶² Id. at 81.

²⁶³ Lemmon v. Snap, Inc., 995 F.3d 1085 (9th Cir. 2021).

²⁶⁴ *Id.* at 1088.

users engaged, Snapchat rewards them with 'trophies, streaks, and social recognitions' based on the Snaps they send."²⁶⁵ Many users, like victims of the crash, believe that sending Snaps that record a 100 mph or faster speed using the Speed Filter will lead to these rewards.²⁶⁶

The boys' parents sued Snap, Inc., alleging that the company encouraged the victims to speed and that the company's negligent app design caused the victims' deaths.²⁶⁷ Snap, Inc. moved to dismiss the parents' claim under § 230, arguing that the harm arose from Snapchat's posting of third-party content on its platform.²⁶⁸ The district court agreed and dismissed the action for failure to state a claim;²⁶⁹ however, the Ninth Circuit reversed, holding that the claim was not barred by § 230.²⁷⁰ The Ninth Circuit rejected the argument that the parents sought to hold Snap, Inc. responsible as a publisher or speaker; rather, the court found that they merely sought to "hold Snapchat liable for its own conduct, principally for *the creation* of the Speed Filter."²⁷¹ Specifically, the parents sought to hold Snap, Inc. liable for its allegedly "unreasonable and negligent" design decisions by which the Speed Filter and the incentive system "worked in tandem to entice young Snapchat users to drive at speeds exceeding 100 MPH."²⁷² Rather than challenge the content of the communications, the parents' claims sounded in traditional principles of products liability law:

The Parents thus allege a cause of action for negligent design—a common products liability tort. This type of claim rests on the premise that manufacturers have a "duty to exercise due care in supplying products that do not present an unreasonable risk of injury or harm to the public."

• • • •

It is thus apparent that the Parents' amended complaint does not seek to hold Snap liable for its conduct as a publisher or speaker. Their negligent design lawsuit treats Snap as a products manufacturer, accusing it of negligently designing a product (Snapchat) with a defect (the interplay between Snapchat's reward system and the Speed Filter). Thus, the duty that Snap allegedly violated "springs from" its distinct capacity as a product designer. This is further evidenced by the fact that Snap could have . . . [taken] reasonable measures

²⁶⁵ Id.

²⁶⁶ Id. at 1089.

²⁶⁷ Id. at 1087.

²⁶⁸ Id. at 1090.

²⁶⁹ Id.

²⁷⁰ Id. at 1087.

²⁷¹ Id. at 1093 (quoting Maynard v. Snapchat, Inc., 816 S.E.2d 77, 81 (Ga. Ct. App. 2018)).

²⁷² Id. at 1091–92.

LEWIS & CLARK LAW REVIEW to design a product more useful than it was foreseeably dangerous-without

altering the content that Snapchat's users generate.²⁷³

However, the same month that the Ninth Circuit in Lemmon restricted § 230 to exempt products liability claims, the Texas Supreme Court in In re Facebook, Inc.²⁷⁴ reached an opposite conclusion. The plaintiffs, three minor girls, alleged they were victims of sex trafficking and became "entangled" with their abusers through Facebook.²⁷⁵ In each case, the plaintiffs alleged that they were contacted on Facebook or Instagram by adult males, groomed to send naked photographs which were sold over the internet, and ultimately lured into sex trafficking.²⁷⁶ The plaintiffs sued Facebook, Inc. under state common law negligence claims, statutory claims prohibiting the sexual exploitation of minors, and products liability claims under the theory that "[a]s a manufacturer, Facebook is responsible for the defective and unreasonable characteristics in its ... product[s]," contending that these products were "marketed to children under the age of 18, without providing adequate warnings and/or instructions regarding the dangers of 'grooming' and human trafficking."277 Following the district court's rulings, Facebook, Inc. sought mandamus relief in the court of appeals to dismiss the entire action under § 230. The Texas Supreme Court permitted the plaintiffs' statutory human-trafficking claims, but dismissed their common law negligence and products liability claims.²⁷⁸

The plaintiffs argued that: "their common-law claims do not treat Facebook as a 'publisher' or 'speaker' because they 'do not seek to hold the company liable for exercising any sort of editorial function over its users' communications."279 The

²⁷³ Id. at 1092 (first quoting LEWIS BASS, PRODUCT LIABILITY: DESIGN AND MANUFACTURING DEFECTS § 2.5 (2d ed. Supp. 2020); and then quoting Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1107 (9th Cir. 2009)).

²⁷⁴ In re Facebook, Inc., 625 S.W.3d 80 (Tex. 2021), cert. denied sub nom. Doe v. Facebook, Inc., 142 S. Ct. 1087 (2022).

²⁷⁵ In re Facebook, Inc., 625 S.W.3d at 82–84.

²⁷⁶ Id. at 84-85. One of the plaintiffs described her ordeal as follows:

Plaintiff was fourteen years old in 2017 and was a user of both Facebook and Instagram, which Facebook owns. She was contacted via Instagram by a male user who was "well over" eighteen years of age. Using "false promises of love and a better future," he lured Plaintiff "into a life of trafficking through traffickers who had access to her and sold her through social media." Her traffickers used Instagram to advertise Plaintiff as a prostitute and to arrange "dates' (that is, the rape of [Plaintiff] in exchange for money)." As a result, Plaintiff was raped numerous times. Following Plaintiff's rescue from the trafficking scheme, traffickers continued to use her profile to attempt to entrap other minors in the same manner. Plaintiff's mother reported these activities to Facebook, which never responded.

Id. at 84.

²⁷⁷ Id. at 85.

²⁷⁸ Id. at 83, 85-86.

²⁷⁹ Id. at 93.

Texas Supreme Court followed *Zeran* and "abundant judicial precedent" in concluding that the duty that the plaintiffs alleged Facebook, Inc. to have violated derived from Facebook's protected status as a publisher or speaker of that content.²⁸⁰ Based upon this reasoning, the Texas Supreme Court concluded that the plaintiffs' products liability claims were similarly barred by § 230:

Plaintiffs' products-liability claims are likewise premised on the alleged failure by Facebook to "provid[e] adequate warnings and/or instructions regarding the dangers of grooming and human trafficking" on its platforms. Like Plaintiffs' other common-law claims, these claims seek to hold Facebook liable for failing to protect Plaintiffs from third-party users on the site. For that reason, courts have consistently held that such claims are barred by section 230. This has been the unanimous view of other courts confronted with claims alleging that defectively designed internet products allowed for transmission of harmful third-party communications.²⁸¹

In reaching this holding, the Texas Supreme Court was clearly sympathetic to the plaintiffs' legal arguments, citing favorably to Thomas's dissent from the denial of certiorari in *Malwarebytes*.²⁸² However, because both statutory interpretations were possible, the court declined to part ways with federal appellate courts.²⁸³

The call by the Texas Supreme Court for a more restrictive interpretation of § 230 was taken up by a bipartisan assembly of 24 state attorney generals who filed an amicus brief in support of certiorari.²⁸⁴ The amici argued that because failure-to-warn and products liability claims do not rely on Facebook Inc.'s status as a publisher or speaker, § 230 does not bar the plaintiffs' claims.²⁸⁵ Nevertheless, the Supreme Court denied certiorari on March 7, 2022.²⁸⁶

In his statement respecting the denial of certiorari, while agreeing that review was premature, Thomas excoriated the broad construction of § 230:

[T]he Texas Supreme Court afforded publisher immunity even though Facebook allegedly "knows its system facilitates human traffickers in identifying and cultivating victims," but has nonetheless "failed to take any reasonable steps to mitigate the use of Facebook by human traffickers" because doing so

²⁸⁰ Id. at 90–93 (citing Force v. Facebook, Inc., 934 F.3d 53, 64 (2d Cir. 2019)).

²⁸¹ Id. at 94.

²⁸² Id. at 90–91 (construing Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13 (2020) (Thomas, J., statement respecting denial of certiorari)).

²⁸³ Id. at 91.

²⁸⁴ Brief for the State of Texas and 24 Other States as Amici Curiae in Support of Petitioner, Doe v. Facebook, Inc., 142 S. Ct. 1087 (2022) (No. 21-459).

²⁸⁵ Id. at 2.

²⁸⁶ Doe v. Facebook, Inc., 142 S. Ct. 1087 (2022) (No. 21-459).

would cost the company users-and the advertising revenue those users generate.287

Once again, he urged his colleagues to clarify § 230's scope "in an appropriate case."288 Seven months later, the U.S. Supreme Court granted certiorari in Gonzalez.²⁸⁹

C. Recent Developments in Social Media Products Liability Litigation

In denying certiorari in Facebook, the U.S. Supreme Court foreclosed the prospect of a swift and definitive resolution of whether products liability claims against social media companies are preempted under § 230. Nevertheless, although not expressly pleaded as a products liability case, Gonzalez will furnish an opportunity for the Court to consider whether algorithmic recommendations are protected publishing activity under § 230. The ruling anticipated in the spring of 2023,²⁹⁰ will be instructive-if not dispositive-on the growing number of products liability cases pending against social media platforms.

Since January 2022, over 100 products liability cases have been filed in state and federal courts throughout the United States against social media companies in cases involving children injured or killed through social media addiction and abuse.²⁹¹ These cases are brought on behalf of minors who fell victim to suicide, accidental death, attempted suicide, suicidal ideation, eating disorders, severe anxiety and depression, racial profiling, sexual abuse, and sex trafficking, in connection with their social media use; in all cases, the plaintiffs renounce any claim based on the social media platforms' status as a publisher or distributor of third-party content.²⁹² The complaints assert both design defect claims, identifying numerous design defects in the algorithms that power the defendants' social media platforms, as

²⁸⁷ Id. at 1088 (Thomas, J., statement respecting denial of certiorari) (citations omitted). ²⁸⁸ Id.

²⁸⁹ Gonzalez v. Google LLC, No. 21-1333, 2022 WL 4651229 (U.S. Oct. 3, 2022).

²⁹⁰ Gonzalez v. Google LLC, SCOTUSBLOG, https://www.scotusblog.com/case-files/cases/ gonzalez-v-google-llc/ (last visited Nov. 20, 2022).

²⁹¹ See, e.g., In re Soc. Media Adolescent Addiction/Pers. Inj. Prods. Liab. Litig., MDL No. 3047, 2022 WL 5409144, at *3 sched. A (J.P.M.L. Oct. 6, 2022).

²⁹² See, e.g., Complaint at 10–11, Rodriguez v. Meta Platforms, Inc., No. 3:22-cv-00401 (N.D. Cal Jan. 22, 2022) (products liability action involving suicide of 11-year-old girl who became addicted to social media at age 9 and suffered sexual exploitation and bullying online); Complaint at 13-15, Doffing v. Meta Platforms, Inc., No 1:22-cv-00100 (D. Or. Jan 20, 2022) (products liability action involving 15-year-old girl with numerous mental health conditions resulting in multiple inpatient psychiatric admissions, eating disorder, self-harm episodes, and physically and mentally abusive behaviors toward family); Complaint at 110-13, Spence v. Meta Platforms, Inc., No 4:22-cv-03294 (N.D. Cal. June 6, 2022) (products liability action involving 13-year-old girl who developed life-threatening eating disorder after becoming addicted to Instagram and being repeatedly directed to content promoting anorexic behavior and negative

well as failure to warn claims, based on the allegedly undisclosed hazards arising from foreseeable product use.²⁹⁸ On October 6, 2022, the U.S. Judicial Panel on Multidistrict Litigation consolidated these cases under 28 U.S.C. § 1407 and transferred them to the Northern District of California before Judge Yvonne Gonzalez Rogers.²⁹⁴ On December 7, 2022, the Judicial Counsel of California coordinated approximately 30 product liability actions pending against social media companies in six California counties pursuant to California Code of Civil Procedure § 404,²⁹⁵ and on January 5, 2023, assigned the coordinated proceeding to Los Angeles County Superior Court, which appointed Judge Caroline Kuhl as the coordination trial judge. As these federal and state consolidated proceedings get underway, the number of similar cases will inevitably increase.²⁹⁶

CONCLUSION

In the two generations that have elapsed since the advent of the internet, the triumphalist ardor over a new world order has been tarnished by the social divisions, political polarization and mental health crises that social media has wrought on our country and our culture. Like the automobile in the early 20th century, the digital transformation is irreversible, and society can no more relinquish social media as it could have dispensed with the automobile in the 1920s. However, just as Cardozo adapted tort law from the stagecoach era to the automotive age,²⁹⁷ legal precedents established when social media did not exist and only 7% of Americans had online access must adapt to an environment where 95% of Americans use social media and online activity animates virtually every aspect of public and private life. The judicial expansion of § 230 beyond its statutory language and legislative mandate was based on a naïve and utopian view of the internet that is wholly irreconcilable with the harsh realities of the current era. The deadly mental health crisis ravaging American

body image); Complaint at 17–23, Smith v. TikTok, Inc., No. 22STCV21355 (Cal. App. Dep't Super. Ct. June 30, 2022) (products liability action for the wrongful death of behalf of two children, ages 8 and 9, who died of self-strangulation after viewing the "blackout challenge" on TikTok).

²⁹³ Complaint at 12–19, *Rodriguez*, No. 3:22-cv-00401; Complaint at 15–27, *Doffing*, No. 1:22-cv-00100; Complaint at 123–33, *Spence*, No. 4:22-cv-03294; Complaint at 23–31, *Smith*, No. 22STCV21355.

²⁹⁴ In re Soc. Media Adolescent Addiction/Pers. Inj. Prods. Liab. Litig., MDL No. 3047, 2022 WL 5409144, at *1, *3 (J.P.M.L. Oct. 6, 2022).

²⁹⁵ See Civil Case Coordination Proceeding (JCCP) Log, JUD. COUNCIL OF CAL., https:// www.courts.ca.gov/documents/CivilCaseCoord_2018toPresent_JCCPLog.pdf (last visited Nov. 20, 2022) (providing case information on JCCP No. 5255 "Social Media Cases" and JCCP No. 5256 "Instagram Cases").

²⁹⁶ Order Assigning Coordinating Trial Judge, Jud. Council Coordinating Proc. Nos. 5255, 5256 (C.D. Cal. Jan. 5, 2023).

²⁹⁷ See MacPherson v. Buick Motor Co., 111 N.E. 1050 (N.Y. 1916).

youth and the pervasive sexual abuse being inflicted on vulnerable children through social media cry out for legal redress. Section 230 can no longer be used as a citadel to protect social media companies from the foreseeable harms and known conse-

quences of their deliberate design decisions.

In the mid-20th century, Justice Traynor saw products liability law as a legal bridge "from industrial revolution to a settled industrial society."²⁹⁸ Today, as Judge Gould observed, products liability law can effectuate a similar transition from the computer revolution to the current post-industrial society by ameliorating the social harms of disruptive social media technologies.²⁹⁹ Application of products liability principles to social media platforms will not throttle free speech, stifle innovation, nor deprive consumers of the tangible benefits that social media provides. Rather, by internalizing safety costs within the economic entities that design and profit from unreasonably dangerous platforms, strict products liability will simply subject social media platforms to the same risk–utility analysis as any other consumer good. And holding social media companies liable for foreseeable harms caused by negligently designed platforms merely imposes the same duty of reasonable care that is born by any other product manufacturer.

Judges and scholars increasingly recognize that the expansive interpretation of § 230 over the past 25 years has incentivized social media companies to elevate profits over public safety, and that products liability provides a sound legal vehicle to promote corporate accountability and consumer safety. In *Gonzalez*, the U.S. Supreme Court is poised to adopt the admonitions of Thomas, Katzmann, Berzon, and Gould, to confine § 230 to its statutory language and legislative intent, and to hold social media companies to the same standard of reasonable care as any other corporate citizen while the Ninth Circuit's holding in *Lemmon* represents the vanguard of this judicial trend. Meanwhile, the hundreds of cases currently being litigated in federal and state courts provide bountiful opportunities for further legal development. To paraphrase Prosser, the assault upon the citadel of § 230 immunity is proceeding in these days apace!³⁰⁰

²⁹⁸ Traynor, supra note 52, at 363.

 $^{^{299}\,}$ Gonzalez v. Google LLC, 2 F.4th 871, 920 (9th Cir. 2021) (Gould, J., concurring in part and dissenting in part).

³⁰⁰ Prosser, *supra* note 75, at 1099.

306

Statement of Matthew P. Bergman Before the Committee on the Judiciary United States Senate

118th Congress, First Session

February 14, 2023



821 Second Avenue Seattle, WA. 98104 (206) 741-4862 matt@socialmediavictims.org

INTRODUCTION

Chairman Durbin and Ranking Member Graham:

Thank you for convening today's hearing Protecting *Our Children Online* and for your bipartisan leadership in promoting Congressional action to address the clear and present danger that unregulated social media platforms poses to the health and safety of America's children.

Fourteen months ago, the U.S. Surgeon General sounded the alarm over the mental health crisis inflicting American youth and the role of social media in contributing to this epidemic.

In these digital public spaces, which [are] privately owned and tend to be run for profit, there can be tension between what's best for the technology company and what's best for the individual user or for society. Business models are often built around maximizing user engagement as opposed to safeguarding users' health and ensuring that users engage with one another in safe and healthy ways. This translates to technology companies focusing on maximizing time spent, not time well spent.

In recent years, there has been growing concern about the impact of digital technologies, particularly social media, on the mental health and wellbeing of children and young people. . . . Importantly, the impact of technology almost certainly varies from person to person, and it also matters what technology is being used and how. So, even if technology doesn't harm young people on average, certain kinds of online activities likely do harm some young people.¹

Unfortunately, in the year since the Surgeon General's clarion call, the youth mental health crisis has not abated, and social media companies continue to elevate their profits over the lives of America's children by failing to implement readily available technologies to make their platforms safer for kids. The time has come for Congress act to hold social media companies the same level of legal accountability as every other company in America. The lives of America's children hangs in the balance.

I. Social Media Victims Law Center Background

I am a lawyer licensed in Washington and Oregon and a 1990 graduate of Lewis & Clark Law School. During law school, I served for one year as a Judicial Extern to Judge Diarmuid F. O'Scannlain of the United States Court of Appeals for the Ninth Circuit. Following graduation from law school, I served for two years as law clerk to Judge Bobby R. Baldock of the United States Court of Appeals for the Tenth Circuit. After completing my clerkship, I worked for four years as a litigation associate at Heller Ehrman White & McAuliffe where my work involved defense of companies facing asbestos liabilities, environmental insurance coverage and Indian law. Since 1995, I have represented victims in product liability cases in state and federal court.

¹ U.S. SURGEON GEN., ADVISORY: PROTECTING YOUTH MENTAL HEALTH 25 (2021) (citations omitted)

In addition to my litigation practice, I have been an adjunct professor at Lewis & Clark Law School since 2019 where I teach litigation strategy to upper division students. I serve as Chair of the Lewis and Clark Law School Board of Visitors and on the Executive Committee of the Lewis and Clark Board of Trustees. Outside the legal arena, I serve on board of the bipartisan American Security Project and the American Jewish Committee's Arabian Gulf Institute.

In the fall of 2021, I founded Social Media Victims Law Center (SMVLC) in response to the mental health epidemic ravaging American youth to advocate for parents of children injured or killed through social media addiction and abuse. After 25 years of representing tort victims in complex product liability cases, I wanted to devote the remainder of my legal career applying this litigation experience towards protecting children from becoming victims in the first place.

SMVLC is the only law firm in the country exclusively focused on children injured by social media. We currently represent 1,368 parents throughout the United States in cases involving completed suicide, accidental death, attempted suicide, suicidal ideation, eating disorders, severe anxiety and depression, racial profiling, sexual abuse, and sex trafficking.

In January 2022, SMVLC filed the first case in the country to invoke strict product liability against social media companies on behalf of an injured child: *Rodriguez v. Meta Platforms, Inc.*, No. 3:22-cv-00401 (N.D. Cal 2022) (wrongful death action arising from suicide of 11-year-old child). Last September, SMVLC filed the Coordination Petition that resulted in the above-referenced coordinated proceeding. SMVLC currently has 35 cases pending in California state court involving 69 plaintiffs and 32 cases in the federal MDL in the Northern District of California. All these cases involve minors or young adults harmed or killed through social media addiction and abuse. Our cases are not about content, but rather, about the products social media companies design and the programming, and operational decisions they make to keep kids hooked on their platforms.

SMVLC is recognized internationally for our expertise in legal, technical, and scientific issues relating to social media addiction and abuse among minors. I have been an invited speaker at the annual convention of the American Association for Justice, Mass Torts Made Perfect, Harris Martin, and Perrin CLEs. I was the only practicing attorney invited to participate in the First International Digital Wellbeing Summit last March in Dhahran, Saudi Arabia where academics, thought leaders, and computer scientists from around the world discussed the impact of social media on young people.

II. Social Media Platforms are Dangerous by Design

SMVLC represents 1,368 parents whose children sustained the following harms:

Wrongful death $-\underline{89}$ cases, 6.51% Attempted Suicide $-\underline{621}$ cases, 45.39% Self-harm $-\underline{823}$ cases, 60.16% Suicidal Ideation $-\underline{962}$ cases, 70.32% Eating Disorders $-\underline{776}$ cases, 56.73% Unhealthy Concerns with Body $-\underline{1115}$ cases, 81.51%

Severe Depression $-\frac{1209}{200}$ cases, 88.38% Bullying $-\frac{1076}{200}$ cases, 78.65% Exchanged Explicit Photos $-\frac{643}{200}$ cases, 47.00% Sexual Contact With Person Over $18 - \frac{297}{200}$ cases, 21.71% Sex Trafficking $-\frac{68}{200}$ cases, 4.97% Sleep Deprivation $-\frac{954}{200}$ cases, 69.74%

Of the 89 parents whose children have lost their lives, their causes of death are as follows:

Completed Suicide - 59 Accidental Death from TikTok Blackout Challenge - 11 Fentanyl Poisoning from Prescription Drugs Bought Through Snapchat - 28 Accidental Death from Russian Roulette Promoted on Social Media – 1

The foregoing harms are neither a coincidence nor an accident but arise from social media companies' deliberate design decision to elevate user engagement over product safety.

A. Maximizing Engagement Through Addictive Product Design

Maximizing engagement is the primary practice underpinning the business model of the largest social media companies in the United States. Social media companies design their platforms maximize time, activity, and advertising exposure on their platforms in pursuit of astronomical profits. There are many techniques used to extend young people's time and activity on platforms, including rewards such as badges and levels, navigational manipulations such as "dark patterns" and autoplay, content recommender systems and social manipulations. Platforms such as Meta, Snap and TikTok extract as much personal data² from minors as possible in order to maximize time, activity and advertising exposure on their platforms in pursuit of astronomical profits. The impact of these practices on minors can be devastating, but these companies continue prioritizing their own commercial best interests over children's best interests.³

Young people are so often described as chronic "overusers" of commercial surveillance products, including social media, video streaming sites and games, from social psychologists describing younger generations as the "iGens"⁴ to popular culture references of young people glued to their phones, it's almost become a cliché. But this characterization reflects reality for a great many minors in the United States, who demonstrate overuse, problematic use and even addiction and resulting harm.

Overuse is common; a recent study found that 36 percent of American teenagers aged 13-17 report spending too much time on social media, and 54 percent say it would be hard or very hard to give

4

² Including sensitive personal data, identifiable data and metadata about device and use data.

³ Limited research has explored whether digital designers and developers consider the needs and safety of minors in their production process, and suggests that young people's needs and experiences are largely overlooked. (See Amanda Lenhard & Kellie Owens 2019 *The UnSeen Teen https://datasociety.net/library/the-unseen-teen/* and Revealing Reality 2021 *Pathways: How Digital Design Puts Children at Risk.*

https://www.revealingreality.co.uk/2021/07/20/report-launch-pathways-how-digital-design-puts-children-at-risk/). ⁴ Jean Twenge 2017 *iGen* First Atria, NY.

up social media.⁵ For many young people, this overuse and inability to log off often "tips over" the line into problematic use. Problematic internet use is defined as use that is risky, excessive or impulsive, and associated with adverse life consequences (such as physical, emotional or social or harms). It is a particularly acute issue for minors .

Harmful as problematic internet use is, it is not a psychiatric diagnosis per se, but for some young people diagnosable addiction becomes a problem. An addictive paradigm describes many social media users' behavior,⁶ particularly adolescents, and the Bergen Social Media Addiction Scale⁷ is now widely used by researchers and mental health professionals to identify and quantify addictive social media behavior.⁸

An estimated 8 percent of American children who use the internet and games show signs of clinical addiction.⁹ The rise of social media's popularity since 2013 has also led some clinical researchers to speculate about the addictive behaviors of young social media users.¹⁰

This is not a niche concern, it means that a third of American teens say they spend too much time on social media (overuse), with many of those young people demonstrating problematic social media use that affects their quality of life. While many studies and surveys document the issues experienced by minors themselves, this rise in problematic behavior has not come out of nowhere. Understanding these issues requires a deeper examination of the role of the digital environment that minors inhabit itself.

Leading social media companies have deliberately designed and developed this digital environment in ways that engineer increasing risks across the spectrum (from overuse to problematic use and addiction). This often results in harms ranging from anxiety, depression, sleep deprivation, self-harm, suicidal ideation, to even death. This deliberate engineering is often called "extended use design," or "persuasive design," "sticky design", or "optimizing for time/attention or activity."

Extended use designs are design practices and acts that aim to maximize time & activity the users spend on a platform, and are prevalent across social media, video streaming platforms and online

⁸ See, e.g., Chung-Ying Lin, Anders Broström, Per Nilsen, Mark D. Griffiths & Amir H. Pakpour, Psychometric Validation of the Persian Bergen Social Media Addiction Scale Using Classic Test Theory and Rasch Models, 6 J. BEHAV. ADDICTIONS 620 (2017).

⁵ Pew Research Center 2022 Teens, Social Media and Technology 2022.

https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/

⁶ Hunt Allcott, Matthew Gentzkow & Lena Song, *Digital Addiction* 29 (Nat'l Bureau of Econ. Rsch., Working Paper No. 28936, 2022) (finding that "self-control problems magnified by habit formation might be responsible for 31 percent of social media use").

⁷ Cecilie Schou Andreassen, Torbjørn Torsheim, Geir Scott Brunborg & Ståle Pallesen, Development of a Facebook Addiction Scale, 110 PSYCH. REPS. 501 (2012).

⁹ See Douglas Gentile 2009 "Pathological video-game use among youth ages 8 to 18: a national study" Psychological Science 2009 <u>https://doi.org/10.1111/j.1467-9280.2009.02340.x</u>.

¹⁰ Cecilie Andreassen 2015 "Online social network site addiction: A comprehensive review" Current Addiction Reports <u>https://doi.org/10.1007/s40429-015-0056-9</u> who explores the potential for social networking sites to be addictive.

⁵

games.

As a strategy, extended use design reflects a set of deliberate decisions by social media companies to design and build products in ways that demonstrably extend the amount of time and activity people spend on their products. Understanding the effects of extended use design is a relatively new area of study, but already research suggests that there is cause for concern.

From a psychological perspective, these sorts of design techniques "prompt behavioral, cognitive, psycho-social, and other psychological mechanisms to change a person's attitudes and behavior and, while doing so, they may trigger or expedite mechanisms related to addictive behavior."¹¹ Many of these techniques are refined by and build on these psychological understandings about users' vulnerabilities and weaknesses; they explicitly exploit cognitive vulnerabilities to extend the amount of time and activity young people spend on digital services. Moreover, those involved in the early development of these companies suggest that they were aware of the likely harms they would cause when they began implementing these design decisions. Meta's first President, Sean Parker, in a 2017 interview, said:

God only knows what it's doing to our children's brains. The thought process that went into building these applications, Facebook being the first of them, ... was all about: "How do we consume as much of your time and conscious attention as possible?" And that means that we need 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. And that's going to get you to contribute more content, and that's going to get you ... more likes and comments. It's a social-validation feedback loop ... exactly the kind of thing that a hacker like myself would come up with, because you're exploiting a vulnerability in human psychology. The inventors, creators — it's me, it's Mark [Zuckerberg], it's Kevin Systrom on Instagram, it's all of these people — understood this consciously. And we did it anyway.¹²

These design decisions are business decisions; time and activity are critical commodities of the attention economy that underpins commercial surveillance. Time is important both because it allows digital services and products to serve more advertising to young people, but also because it allows for more activity. Online activity, such as viewing content, commenting, sharing or creating content, allows companies to collect more personal data about young people which they can in turn, use to sell personalized advertising. Time and activity create a treasure trove of data about young people for companies, fueling the business model of commercial surveillance. Extended use design inherently furthers the commercial surveillance of children.

 ¹¹ Deniz Cemiloglu, Mohammad Naiseh, Maris Catania, Harri Oinas-Kukkonen & Raian Ali 2021 "The Fine Line Between Persuasion and Digital Addiction." In:Persuasive Technology <u>https://doi.org/10.1007/978-3-030-79460-</u>
 6 23.

⁶_23. ¹² Mike Allen, Sean Parker unloads on Facebook: "God only knows what it's doing to our children's brains", Axios (November 9, 2017), <u>https://www.axios.com/2017/12/15/sean-parker-</u>

Unloads-on-facebook-god-only-knows-what-its-doing-to-our-childrens-brains-1513306792.

B. <u>Extended Use Design</u>

Social media platforms actively seek out minors to drive growth.¹³ Public disclosures made by the Facebook Whistleblower, and other insiders who have come forth since, confirm as much. "Extended use design" incorporates a number of acts and practices routinely deployed on products and services used by young people, and below, we examine four common practices.

1. Gamification

Gamification – or the use of game design principles outside game contexts¹⁴ – is a technique used to "change behavior in non game settings."¹⁵ Gamification is often deployed to develop features used to drive users to extend, prolong or return to a digital service. These often take the form of low-friction, variable rewards such as:¹⁶

- Badges, icons or stickers or other visual representations reflecting a user's activity levels or use time. For example Snapchat's snapstreak badge that indicates how many days users have "snapped" each other in a row. A special ¹⁰/₂ appears next to the streak if it continues for 100 days. Young people have reported being distraught when their snapstreaks end, with highschoolers talking about the amount of time and effort they invest in maintaining them.¹⁷ Research has shown that badges lead to increased user activity.¹⁸
- Points or rewards can be given to encourage users to use a product or service. Research into
 manipulative design features deployed on children's apps found multiple rewards or "lures"
 designed to encourage child users to stay on or return to games. These included, for example
 "daily rewards in *Green Grandpa Alien*" or rewards users "could earn for repeated play (e.g.,

¹³ Alex Health 2021 "Facebook's lost generation" *The Verge.* www.theverge.com/22743744/facebook-teen-usage-decline-frances-haugen-leaks and David Swan 2021 "Aussie teens dump Facebook" *The Australian.* www.theaustralian.com.au/business/technology/aussie-teens-dump-facebook-instagram-leaked-internal-research-reveals/news-story/3e0a464b67bd5f45ee0fa00b14bfe551 and https://www.cbsnews.com/news/social-media-political-polarization-60-minutes-2022-11-06/ ("In [China's] version of TikTok, if you're under 14 years old, they show you science experiments ... they also limit it to only 40 minutes per day. Now they don't ship that version of TikTok, while they ship the opium version to the rest of the world ... they make their domestic version a spinach version of TikTok, while they ship the opium version to the rest of the world. The version served to the west has kids hooked for hours at a time.").
¹⁴ Karen Robson, Kirk Plangger, Jan Kietzmann, Jan McCarthy & Leyland Pitt 2015 "Is it all a game?

¹⁵ Ian McCarthy, Jan Kietzmann, Karen Robson, Kirk Plangger, and Leyland Pitt 2014 'Understanding Gamification of Consumer Experiences' Advances in Consumer Research

http://www.acrwebsite.org/volumes/1017445/volumes/v42/NA-42.

¹⁶ For a full discussion of different elements of gamification, see Stuart Hallifax Audrey Serna, Jean-Charles, Guillaume Lavoué and Elise Lavoué 'Factors to Consider for Tailored Gamification' CHI PLAY https://doi.org/10.1145/3311350.3347167.

¹⁷ Rachel Thompson 2017 "Devastated Snapchatters talk about the heartbreak of losing a Snapstreak after hundreds of days" *Mashable* <u>https://mashable.com/article/breaking-snapstreak-snapchat-streak;</u> https://abcnews.go.com/Lifestyle/experts-warn-parents-snapchat-hook-teens-streaks/story?id=48778296; <u>https://www.bbc.com/news/technology-47623626</u>.

¹⁸ Juho Hamari 2017 "Do badges increase user activity? A field experiment on effects of gamification." *Computers in Human Behavior*. http://dx.doi.org/10.1016/j.chb.2015.03.036.

⁷

DisneyNow displays types of virtual items players can earn for gameplay targets)" or even sometimes rewards for repetitive play, "*Scribblencuts Remix* offers a gold crown for a repetitive gameplay."¹⁹ Snap Inc. likewise utilizes various hidden reward features, including Snapscores, Trophies, and Charms.

- Leaderboards or rankings are often used to enable social comparison to enhance engagement.²⁰ Leaderboards and rankings can often be displayed at the right time or at the right way to encourage users to continue or extend their engagement. For example, Spotify now notifies fans when they are in the top 1 percent of listeners, implicitly encouraging users to listen to their favorite artists more. At least one artist was known to exploit this, calling anyone not in their top 1 percent a "fake fan."²¹
- Pull to refresh. Most apps can automatically update content, however many have installed a "pull to refresh" feature, where users need to "pull down" and release the screen, before new content pops up. This product feature is based on how slot machines operate. This pull to refresh design induces a ludic-loop (or repeated cycles of uncertainty, anticipation and then feedback, where the rewards are just enough to keep you going),²² and manipulates brain chemistry further by preventing natural end points that would otherwise encourage users to move on to other activities.
- Loot Boxes are purchasable in-game or in-app content with randomized rewards. For example, young video game players can purchase a "mystery box" in a football game that may include their favorite players. Boxes often come with advertised odds, which has raised significant concerns about the structural and psychological similarities with gambling.²³ Loot boxes can cause significant economic harms to minors. A 2020 study of the impact of Loot Boxes found that:²⁴
 - 23 percent of 11- to 16-year-old gamers had paid money to open loot boxes.
 - 31 percent said they struggled to keep track of how much they spent on loot boxes.
 - 33 percent said they did not feel in control of their spending on loot boxes.
 - One in four gamers spend around \$120 on loot boxes on average over the course of a game.
 - 15 percent had taken money from their parents without permission to buy a loot box; and 9 percent had borrowed money they couldn't repay.

 ¹⁹ Jenny Radesky, Alexis Hiniker, Caroline McLaren, Eliz Akgun, Alexandria Schaller, Heidi Weeks, Scott Campbell, Ashley Gearhardt 2022 "Prevalence and Characteristics of Manipulative Design in Mobile Applications Used by Children." *JAMA Open Network* <u>https://doi.org/10.1001%2Fjamanetworkopen.2022.17641</u>.
 ²⁰ Yuan Jia, Yikun Liu, Xing Yu, and Stephen Voida. 2017 "Designing Leaderboards for Gamifications Perceived Differences Based on User Ranking, Application Domain, and Personality Traits" *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. <u>https://doi.org/10.1145/3025453.3025826</u>.

²¹ PopBuzz 2021 "How to find Spotify's 'Top 1% of Fans' Feature" *PopBuzz* https://www.popbuzz.com/music/news/epotify.top.1-fans/

https://www.popbuzz.com/music/news/spotify-top-1-fans/. 22 Natasha Schüll 2014 Addiction by Design Princeton University Press.

²³ James Close & Joanne Lloyd 2020 Lifting the Lid on Loot-Boxes

https://www.begambleaware.org/sites/default/files/2021-03/Gaming_and_Gambling_Report_Final.pdf. ²⁴ Gambling Health Alliance 2020 What Is The Financial Impact Of Loot Boxes On Minors ?

- 11 percent had either used their parent's credit or debit card, or borrowed money from friends or family to do so.
- 24 percent of gamers said they felt addicted to loot boxes and 44 percent said they experienced feelings of frustration and anger more often than they otherwise would have because of the feeling of being cheated or ripped off by loot boxes.
- Push notifications deserve particular attention. Push notifications are clickable, pop-up notifications that digital services and products "push" to users when they are logged off, aiming to pull user's back to the platform. A former Facebook developer outlined that "the vast majority of push notifications are just distractions that pull us out of the moment... They get us hooked on pulling our phones out and getting lost in a quick hit of information that could wait for later, or doesn't matter at all."²⁵ Push notifications exploit users psychological vulnerabilities²⁶ seemingly without end; the average American consumer receives 56 push notifications at day.²⁷ This includes minors , who are often sent push notifications after bed-time,²⁸ which has been implicated in children losing up to 8 hours of sleep a week.²⁹

Cemiloglu *et al*³⁰ document how these sorts of reminders and push notifications are associated with multiple pathways to addiction, including self-regulation theories that suggest that push notifications act as triggers that disrupt people from their primary goals and make it difficult to "log off."³¹ This often results in loss of control and preoccupation with digital products and

²⁵ Justin Rosenstein, co-creator of Facebook's Like Button, in Julian Morgans 2017 "The Secret Ways Social Media Is Built for Addiction" Vice <u>https://www.vice.com/en/article/vv5jkb/the-secret-ways-social-media-is-built-for-addiction</u>.

²⁶For example, they are designed to be psychological triggers that exploit vulnerabilities, such as being sent at times that maximize individuals 'interruptibility' (See Abhinav Mehrotra, Mirco Musolesi, Robert Hendley, and Veljko Pejovic. 2015. 'Designing content-driven intelligent notification mechanisms for mobile applications. In Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing https://doi.org/10.1145/2750858.2807544).

²⁷ See Martin Pielot, Amalia Vradi, and Souneil Park. 2018 "Dismissed! A detailed exploration of how mobile phone users handle push notifications" *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services* <u>https://doi.org/10.1145/3229434.3229445</u>.

²⁸ See Olivia Rudgard 2022 "Stop sending children social media notifications during the night, says privacy expert" The Telegraph <u>https://www.telegraph.co.uk/news/2018/03/22/stop-sending-children-social-media-notificationsnight-says/</u> ²⁹ c. - During the interview and the sender of the

²⁹ See De Montfort University 2022 DMU research suggests 10-year-olds lose sleep to check social media https://www.dmu.ac.uk/research/research-news/2022/dmu-research-suggests-10-year-olds-lose-sleep-to-checksocial-media.aspx#:~:text=Research%20support-

DMU%20research%20suggests%2010%2Dyear%2Dolds%20lose%20sleep%20to%20check.up%20to%20use%20s ocial%20media, where research suggests that up to one in eight 10-year-olds are voluntarily waking themselves in the middle of the night to check their push notifications.

³⁰ Deniz Cemiloglu, Mohammad Naiseh, Maris Catania, Harri Oinas-Kukkonen & Raian Ali 2021 "The Fine Line Between Persuasion and Digital Addiction." In:Persuasive Technology <u>https://doi.org/10.1007/978-3-030-79460-</u> <u>6 23</u>.

 <sup>6 23.
 &</sup>lt;sup>31</sup> See also Jie Du, Peter Kerkhof, and Guido M. van Koningsbruggen 2019 "Predictors of social media self-control failure: Immediate gratifications, habitual checking, ubiquity, and notifications" *Cyberpsychology, Behavior, and Social Networking* https://doi.org/10.1089/cyber.2018.0730.

⁹

services.³² This is notable because "preoccupation" is one of the main symptoms of addiction.³³ Likewise, learning theories of addiction suggest that push notifications act as a trigger for the expectation of a positive experience:

For instance, if a person checks his or her Facebook profile each time he or she receives a notification from Facebook and learns that this is enjoyable, then over time the user would have formed the habit of checking every notification that is received from Facebook. Consequently, the user will automatically check his or her Facebook profile the next time a notification comes in without paying any regard to the appropriateness of the action. Indeed, habits drive addictions symptoms.³⁴

These specific game-style elements have been shown to have psychological effects on users,³⁵ that differ between users including younger users.³⁶ They are often used in social media services and other digital products frequently used by minors ³⁷ to extend use. Research exploring the prevalence of design abuses in common children's games in the U.S., found that gamification lures designed to extend use were found in 45.1 percent of children's apps analyzed.³⁸ Cemiloglu *et al*³⁹ document how these sort of gamified rewards are associated with multiple pathways to addiction, from biological theories that suggest rewards provide a dopamine hit to learning theories that suggest they are an addictive form of reward. Likewise a letter to the American Psychological Association, signed by 50 psychologists, note that the use of rewards, such as badges and leaderboards

take advantage of the inherent developmental drive in preteen and teen boys to gain competencies, or abilities that have helped them throughout history become evolutionarily successful. Psychologists and other UX researchers create video games with powerful

³² Robert LaRose, Carolyn A. Lin & Matthew S. Eastin, 2003 "Unregulated Internet usage: Addiction, habit, or deficient self-regulation?." *Media psychology* https://doi.org/10.1207/S1532785XMEP0503_01.

³³ Deniz Cemiloglu, Mohammad Naiseh, Maris Catania, Harri Oinas-Kukkonen & Raian Ali 2021 "The Fine Line Between Persuasion and Digital Addiction." In:Persuasive Technology <u>https://doi.org/10.1007/978-3-030-79460-</u> 6 23.

^{6 23.} ³⁴ Babajide Osatuyi & Ofir Turel 2018 "Tug of war between social self-regulation and habit: Explaining the experience of momentary social media addiction symptoms" *Computers in Human Behavior* <u>https://doi.org/10.1016/j.chb.2018.03.037</u>.

³⁵ Michael Sailer, Jan Ulrich Hense, Sarah Katharina Mayr, Heinz Mandl 2017 "How gamification motivates: An experimental study of the effects of specific game design elements on psychological need satisfaction" *Computers in Human Behavior* <u>http://dx.doi.org/10.1016/j.chb.2016.12.033</u>.

³⁶ Although the impact of gamification on children and teenagers is uniquely understudied. For example, a systematic review in 2020 found only four studies that explored impact by age (See Ana Carolina Tomé Klock, Isabela Gasparini, Marcelo Soares Pimenta, Juho Hamari 2020 "Tailored Gamifications: A review of literature" *International Journal of Human Computer Studies* <u>https://doi.org/10.1016/j.ijhcs.2020.102495</u>.

³⁷ Gokhan Aydin 2015 "Adoption of Gamified Systems: A Study on a Social Media Gamification Website." *LJOM* <u>http://doi.org.ezproxy-b.deakin.edu.au/10.4018/IJOM.2015070102.</u>

³⁸ Jenny Radesky, Alexis Hiniker, Caroline McLaren, Eliz Akgun, Alexandria Schaller, Heidi Weeks, Scott Campbell, Ashley Gearhardt 2022 "Prevalence and Characteristics of Manipulative Design in Mobile Applications Used by Children." JAMA Open Network <u>https://doi.org/10.1001%2Fjamanetworkopen.2022.17641</u>.

³⁹ Deniz Cemiloglu, Mohammad Naiseh, Maris Catania, Harri Oinas-Kukkonen & Raian Ali 2021 "The Fine Line Between Persuasion and Digital Addiction." In:Persuasive Technology <u>https://doi.org/10.1007/978-3-030-79460-6_23</u>.

¹⁰

rewards doled out on intermittent schedules that convince kids, especially adolescent boys, that they are mastering important competencies through game play.⁴⁰

2. Life Examples of Addictive Social Media Behavior

These sorts of rewards can cause psychological harm. Emi, an 18-year-old, describes how stories, push notifications and other extended use design features affected their sense of psychological well-being (see Appendix A:1 for their full story).

The longer I scrolled on Instagram or watched Snapchat Stories, the more I'd see "Instagram girls" from my school — the lucky ones who could choose how exactly they wanted their hair to look and had the long, flowing hair to do it. I kept logging in because I wanted to fit in, and on social media it felt like it was possible to fit in, if you got enough likes you could be successful and popular. So I kept logging in, I couldn't help but want to be successful and popular. But this was also the time that Instagram stories came out, and when someone uploaded a new story there would be a push notification. And I'd get this notification that one of my classmates or one of my friends had a new story. I'd click on the notification and get sent yet another story that made me feel like I couldn't fit in.

They can also be persistent and encourage problematic use and addiction.

G.D. opened social media accounts around age 11 or 12, without her parents' knowledge or consent. One time her father convinced her to leave her phone in the car while they went shopping. It was a struggle but she did. They were in the store for maybe an hour and when they got back to the car G.D. had roughly 300 new notifications from Instagram, Snapchat, and TikTok. She had been off their product for less than 60 minutes and all three flooded her with messages like "look what you missed while you were gone." G.D. struggles to put her phone down because of these notifications and cannot put it down for more than a few minutes before the constant ping of notifications begins.⁴¹

Another parent described the harms push notifications were creating for their child.

Snapchat also makes sure that I can't keep [my child] off the phone for very long, in more than one way. For example, every time she puts the phone down it buzzes. One night I took the phone away and it was like a slot machine in my drawer, going off constantly with push notifications from Snap and Instagram. I saw them in the morning, multiple Snapchats notifications and my mind was blown with the sheer number, which was easily dozens if not over a 100 new snap messages. Snap and Instagram were sending her push notifications all night long. And when I take the phone away, Snap and Instagram then send her emails telling her when she gets a

⁴⁰ ScreenTime Network Our Letter to the APA <u>https://screentimenetwork.org/apa</u>.

⁴¹ D.D. et al. v. Meta Platforms Inc. et al., U.S. District Court for the Northern District of California, Case No. 3:22cv-06190 (filed October 19, 2022) ("D.D. Complaint").

¹¹

new message on their social media app, or a friend has done something. One time, she had 18 emails from Snap and Instagram with these types of notifications, and it caused huge issues. It's like dangling heroin in front of a heroin addict, and triggers her all over again.42

The harms to minors associated with these low-friction rewards can ultimately become tragic, physical harms. For example, for Brantley, a 17-year-old man, his addictive behaviors ultimately became lethal. His family describe how his problematic use was initially fueled by push notifications (See Appendix B:1).

In May of 2019, Brantley got a new phone and immediately began receiving Facebook's push notifications - designed to keep him on the app - at all hours of the day and night. Brantley began accessing Facebook every chance he got, to the point where he no longer slept. ... Shortly after Brantley had access to Facebook on his phone he also began staying awake until 3 and 4 am engaged with the Facebook product. Meta tracks all usage and was aware of Brantley's excessive and dangerous use of its product, while his own parents were not, and had no way to ascertain such problematic use since Brantley appeared to be sleeping whenever his mother passed by his room. As a result of Facebook's engineered addiction, Brantley suffered from severe sleep deprivation and anxiety so extreme that it manifested in physical symptoms like shortness of breath and chest pain.

A 2021 poll found that 84 percent of parents support banning the use of badges that reward kids and teens for increasing their time spent on a platform and 87 percent support banning the use of push notifications to increase kids and teens engagement.43

3. Navigational manipulations

The user journeys or "navigations" available to young people within a digital product or service can also be constructed in ways that manipulate young users into spending more time and activity on a platform. An "endless scroll" is a common navigation feature designed to maximize time and activity. Where a feed has no discernable ending, it is described as endless, which removes any "natural break" triggers that may encourage users to log off.

Instagram presents the perfect example of how deliberate design decisions have been made around "endless scrolling" in order to manipulate users' time and activity. In 2018, to help address problems arising from "the endless scroll," Instagram introduced a feature that provided users a notification when they had scrolled so far that they had seen all the new content from the people they followed. A notification that said "you're all caught up" would appear, functioning as a

⁴² Brittney Doffing v. Meta Platforms, Inc. et al., U.S. District Court for the District of Oregon, Case No. 1:22-cv-00100-CL (filed January 20, 2022) ("Doffing Complaint," "Doffing Declaration," "Findings and Recommendation"); see Doffing Declaration, 34-35.

Accountable Tech 2021 Accountable Tech Frequency Questionnaire 2021 https://accountabletech.org/wpcontent/uploads/Accountable-Tech-Parents-Poll.pdf.

natural trigger to "end" a session on Instagram.⁴⁴ However, in 2020 with extensive competition from TikTok, Instagram introduced content from recommender algorithms at the end of the feed, meaning that people could scroll endlessly and see new content - in other words, you never "catch up" no matter how long you watch because there is always more content to see.⁴⁵ More recently, they changed this again by introducing suggested content into the feed (rather than simply at the end of the feed), making "endless scrolling" even more inevitable.⁴⁶ Without a natural end to the scroll, young people must rely on their self-regulation and willpower to log off.

In order to keep young people watching, engaging or playing more, many digital products design friction-free movement from one piece of content to the next. This automatic movement is designed to reduce the "trigger" for users to disconnect at what might otherwise feel like a natural break, or to maximize a user's "flow."⁴⁷

For example, on video streaming sites like YouTube or TikTok, videos may be cued up to play one after the other. Without a trigger to prompt users to stop, it is really easy to spend more time than intended on these platforms. Researchers from the University of Kent describe how without these sorts of triggers or external barriers to stop, without realizing it, 10 minutes can become an hour or two on video streaming platforms, which parallels addictive patterns.⁴⁸ Autoplay leads to overstimulation, which research has shown to affect people's "internal clocks" when using social media; people consistently underestimate the amount of time that has passed on social media sites because they receive too much stimulus.⁴⁹

In games, auto-advancing often discourages minors from logging off, and locks them into playing the next level. For example, games might only provide a "play next level" button at the end of one level, with no clear way to navigate back to the home page or end. Navigational constraints such as auto-advancing to extend gameplay was found in 45.9 percent of children's apps analyzed.⁵⁰

⁴⁴ Instagram 2018 "Introducing You're all Caught Up!"

https://about.instagram.com/blog/announcements/introducing-youre-all-caught-up-in-feed.

⁴⁵ Sarah Perez 2020 "Instagram finds new ad space at the end of your feed with launch of 'Suggested Posts' feature" *TechCrunch* <u>https://techcrunch.com/2020/08/19/instagram-finds-new-ad-space-at-the-end-of-your-feed-with-launch-of-suggested-posts-feature/.</u>

⁴⁶ Taylor Hatmaker 2020 "Instagram's newest test mixes "Suggested Posts" into the feed to keep you scrolling" TechCrunch <u>https://techcrunch.com/2021/06/23/instagram-suggested-posts-test-topics/</u>.

⁴⁷ For a description of flow, see Mihaly Csikszentmihalyi & Mihaly Csikzentmihaly 1990 Flow: The psychology of optimal experience New York: Harper & Row.
⁴⁸ Largers Conidic in Linders Deduce WW, 2017 Linders Linde

⁴⁸ Lazaros Gonidis in Lindsay Dodgson "Why TikTok makes the hours seem to melt away, according to experts who study how our brains perceive time" *Insider*. <u>https://www.insider.com/why-time-passes-so-quickly-scrolling-on-tiktok-2022-7</u>. Likewise, researchers exploring social video apps have noted that "a perceived minute" may "actually take several hours in real life" Qing Huang, Mingxin Hu, Ning Zhan 2002 "A techno-psychological approach to understanding problematic use of short-form video applications: The role of flow." *Frontiers in Psychology* <u>https://doi.org/10.3389%2Ffpsyg.2022.971589</u>.

⁴⁹ Lazaros Gonidis & Dinkar Sharma 2017 "Internet and Facebook related images affect the perception of time" *Journal of Applied Social Psychology* <u>https://doi.org/10.1111/jasp.12429</u>.

⁵⁰ Jenny Radesky, Alexis Hiniker, Caroline McLaren, Eliz Akgun, Alexandria Schaller, Heidi Weeks, Scott Campbell, Ashley Gearhardt 2022 "Prevalence and Characteristics of Manipulative Design in Mobile Applications Used by Children." JAMA Open Network <u>https://doi.org/10.1001%2Fjamanetworkopen.2022.17641</u>.

Cemiloglu *et al*⁵¹ document how endless scroll, autoplay and auto-advancing, as systems that reduce the effort users need to expend, conform with biological and self-regulation theories of addiction; autoplay increases the amount of self-control and self-regulation needed to stop. From a biological perspective of addiction, Gonidis notes "when (users) first start using the app, they may watch five videos. But over time, those five videos will no longer be enough to get the same dopamine hit."⁵² This means more and more self-regulation may be needed to log off in the face of an endless scroll or auto-advancing to the next level.

A 2021 poll found that 86 percent of parents support rules requiring that autoplay be turned off by default on platforms with video content aimed at kids.⁵³

While monopolizing young users' time is the main aim of extended-use design, time itself can also be a tool deployed in this process. Time is often used to extend or prolong use, in differing ways. Firstly, "time" can be removed or voided from products to encourage extended use. For example, social media site TikTok removes all markers of time from videos posted, such as dates and times created, which can make TikTok feel like a "timeless" world for users.⁵⁴ Likewise, features that are intended to allow users to "master their time" can be manipulated to keep users logged on longer. For example, in 2021, Instagram began allowing users to set daily time limits as low as 10 or 15 minutes. Earlier this year, Meta changed its settings so that users can now only set a daily limit of 30 minutes or more.⁵⁵

Time can also be exaggerated to create pressure to extend use. For example, including visual clocks that "tick down" or suggest that time is running out to finish a level or save a character can encourage minors to stay on and "beat the clock." These sorts of manipulative techniques are often deployed. In a study of design abuses in children's apps, time pressure was used to prolong gameplay in 17.3 percent of games. These sorts of time pressures are known to interfere with adult's decision-making processes,⁵⁶ so it is likely that these also affect young people's decision-making processes.

https://techcrunch.com/2022/02/21/instagram-limits-daily-time-

⁵¹ Deniz Cemiloglu, Mohammad Naiseh, Maris Catania, Harri Oinas-Kukkonen & Raian Ali 2021 "The Fine Line Between Persuasion and Digital Addiction." *Persuasive Technology* <u>https://doi.org/10.1007/978-3-030-79460-6_23</u>.
⁵² Lazaros Gonidis in Lindsay Dodgson "Why TikTok makes the hours seem to melt away, according to experts who study how our brains perceive time" *Insider* <u>https://www.insider.com/why-time-passes-so-quickly-scrolling-ontiktok-2022-7</u>.

⁵³ Accountable Tech 2021 Accountable Tech Frequency Questionnaire 2021 <u>https://accountabletech.org/wpcontent/uploads/Accountable-Tech-Parents-Poll.pdf.</u>

 ⁵⁴ See Louise Matsakis 2019 "On TikTok, There Is No Time" Wired <u>https://www.wired.com/story/tiktok-time/.</u>
 ⁵⁵ See Natash Lomas 2022 "Instagram quietly limits 'daily time limit' option" TechCrunch

limits/#:~-text=This%20daily%20time%20limit%20setting_out%20of%20the%20app%20voluntarily.
⁵⁶ For example, in an experimental game, adults were asked to make economic decisions in high and low time pressure environments. payoffs are higher under low time pressure than under high time pressure. (See Marti Kocher & Matthias Sutter 2006 "Time is money—Time pressure, incentives, and the quality of decision-making" Journal of Economic Behavior & Organization https://doi.org/10.1016/j.jebo.2004.11.013), or in a driving simulator experiment, perceived time pressure impacted driving decisions. (See Elizabeth Rendon-Velez, Peter van Leeuwen, Reindeer Happee, Inne Horváth, Wilhelm van der Vegte, Joost de Winter, 2016 "The effects of time pressure on driver performance and physiological activity: A driving simulator study." Transportation Research Part F: Traffic Psychology and Behaviour 41 (2016): 150-169. https://doi.org/10.1016/j.jtf2.016.06.013 1369-8478().

They can also result in psychological harms, especially sleep deprivation. Research has shown that increased screen time among children correlates with adverse sleep outcomes,⁵⁷ and many SMVLC clients report endlessly scrolling on social media late at night and difficulty tracking how long they have been online.

At SMVLC, 67 percent of our clients report sleep deprivation in their children as a result of social media, but we are finding after speaking with clients and their children that sleep deprivation is involved in virtually every case. The discrepancy, we believe, is in part because many parents do not realize that their children are unable to sleep and access social media products at night.⁵⁸ In some cases, parents require the phone to be kept in a central location in the home, but young people simply wait until parents are asleep to take and use the device. In others, young people get a secondary device from a friend, a disabled household device with wi-fi access (which most consumers do not realize can be used for social media),⁵⁹ or can even purchase their own device online without parents knowing.⁶⁰

In other cases, young people simply are not exhibiting sleep deprivation symptoms. But in almost every case where we speak with young people directly, or are able to access historical social media data after a young person's death, we find evidence that they were accessing social media during hours when they should have been asleep and, also, when their parents believed that they were asleep.

Likewise, now 20-year-old Alexis Spence talks about the impact of endless scrolls on her psychological well-being.

The endless scrolling on Instagram was one of the most addictive features for me. I was accessing Instagram without my parents knowing as they were not okay with me using social media, and when I was able to get access to it I would often just sit there and scroll through the never ending posts, advertisements, and videos Instagram provided on my Explore page – which over time, were almost entirely pictures, ads, and videos of super skinny women, thigh gaps, visible clavicles, and how-to videos about limiting calories, not eating, losing weight, anorexia, and similar. I could spend literally all night without posting or talking to other users, but just scrolling through the never-ending stream of what Instagram wanted to show me. The way it works is that you can either look at several pieces of content

⁵⁹ See J.S. et al. v. Meta Platforms, Inc. et al., California Superior Court for the County of Yolo, Case No. CV2022-1472 (filed August 26, 2022) ("J.S. Complaint"), ¶¶ 211, 246 (siblings took grandmother's old cell phone device and accessed social media via the wi-fi feature for months and in the middle of the night).

⁵⁷ Lauren Hale & Stanford Guan 2015 "Screen time and sleep among school-aged children and adolescents: A systematic literature review" *Sleep Medicine Reviews* <u>https://doi.org/10.1016/j.smrv.2014.07.007</u>.

⁵⁸ Research has also shown that it is extremely common for teens to use social media at night without their parent's knowledge. (See Elizabeth Englander 2014 "Awake, online and sleep-deprived – the rise of the teenage 'vamper'" *The Conversation* <u>https://theconversation.com/awake-online-and-sleep-deprived-the-rise-of-the-teenage-vamper-34853 & Laura M. Holson 2014 "Social Media's Vampires: They Text by Night" *New York Times* 1457. (2014) [2014] [</u>

http://www.nytimes.com/2014/07/06/fashion/vamping-teenagers-are-up-all-night-texting.html).

⁶⁰ See A.C. et al. v. Meta Platforms, Inc. et al., California Superior Court for the County of Los Angeles, Case No. 22STCV36188 (filed November 15, 2022) (A.C. COMPL, ¶ 96 (11-year-old purchased a phone off eBay with a gift card received for his birthday to regain access to Instagram)).

¹⁵

on the Explore page or click on one piece of content which expands and, from there, you can simply scroll up through image after image after image. You don't even have to search or look for anything because Instagram just feeds you everything in one location, and it never ends. It is so incredibly hard to look away even for a few minutes. You never reach a stopping point or even a break in the flow of rapid-fire content - just never ending photos, advertisements, and videos that keep you glued to the phone and scrolling up for more. It was impossible for me to spend a few minutes scrolling, even when I knew that I needed to do other things or go to sleep. What I intended to be just a few minutes would almost always turn into hours and hours of non-stop scrolling – time I didn't mean to spend – when I was supposed to be doing other things.

C. Algorithmic Recommendation of Unwanted and Dangerous Content

The manner in which content is presented to users can maximize use and activity, such as endless scroll and autoplay. But which content is chosen for users to view can also be maximized to use and activity. Content recommender systems, underpinned by machine learning algorithms, determine which content users are presented with. They have been described as "one of the most effective ways that platforms can keep users clicking and viewing ads on their site to the tune of billions of dollars in revenue."⁶¹

These algorithms are sophisticated in terms of their mathematics; they perform multiple analyses and experiments each second determining and learning which content users are most likely to watch or interact with. While they may be mathematically smart, they are obtuse when it comes to impact and rely entirely on the humans programming them to make safety-related decisions. These algorithms do not distinguish between helpful or harmful content they direct to minors or the consequences of consistently connecting users with content chosen solely to increase minors' engagement with their the social media product. Rather, social media companies knowingly harness operant conditioning methodologies to artificial intelligence to maximize minors' engagement at the expense of their physical safety and psychological well-being. For example, Google trains its YouTube algorithms to connect and expose users to videos that maximize the amount of time they watch YouTube, regardless of what the content is or how long someone has been watching.⁶² TikTok likewise programs and operates its algorithms "to optimize for two closely related metrics in the stream of videos it serves: "retention" - that is, whether a user comes

⁶¹ Allison Zakon 2019 "Optimized for Addiction: Extending Product Liability Concepts to Defectively Designed Social Media Algorithms and Overcoming the Communications Decency Act" *Wisconsin Law Review* <u>http://dx.doi.org/10.2139/ssm.3682048</u> pp.7.

⁵² Kevin Roose 2019 "The Making of a YouTube Radical" New York Times

https://www.nytimes.com/interactive/2019/06/08/technology/voutube-radical.html, who describes how in 2021 "YouTube's executives announced that the recommendation algorithm would give more weight to watch time, rather than views. That way, creators would be encouraged to make videos that users would finish, users would be more satisfied and YouTube would be able to show them more ads."

back - and "time spent." The app wants to keep you there as long as possible."⁶³ The results have been described as algorithms "optimized for addiction."⁶⁴

Most companies tell consumers that they program their recommendation technologies to send users content of likely interest; in fact, however, and as will be illustrated through the summaries of just a few of our cases below, this is often not what social media companies are doing. Rather, they deliberately program their algorithms to connect and expose minors to content, subject matters, and even other users *they do not want and in which they have no interest*.

For example, content recommended systems have been shown to consistently push young women eating disorder content⁶⁵ to maximize engagement, causing serious harm. Kelsey, a 17-year-old, describes how the content recommender system flooded her feed with dangerous weight-loss content just so she would stay online longer. (See Appendix A:2).

As someone who had grown up with Instagram, I can't recall a time when the app <u>didn't</u> show me this sort of dangerous content. I felt like Instagram's and its algorithms were always populating my feed with it, almost from the moment I created my account... At one point, it got so normalized that prominent figures like the Kardashians were openly promoting weight loss supplements and diet suppressors. I hadn't had an interest in these things and yet they'd pop up on my screen like magic.

Alexis Spence was 11 when she opened her first Instagram account, and was also flooded with eating disorder content. (See Appendix B:2, <u>Spence Complaint</u>).

For years, Meta flooded Alexis's Explore page with thigh gaps and models that were skinny to the point of illness. Meta likewise recommended and connected her with other (often adult) users and influencers suffering from disordered eating, as well as groups and group members who then encouraged Alexis in her eating disorder and self-harm.

The relentlessness of an algorithm programmed to not just thoughtlessly push content onto young people, but to push content designed to keep their attention at any cost can quickly escalate into tragic physical harm. For example, Chase, a 16-year-old man took his life after TikTok decided to maximize his engagement by sending him male pain, suicide and self-harm content - even though Chase himself was asking TikTok to send him motivational speeches and encouragement instead. (See Appendix B:3, Nasca Complaint).

⁶³ Ben Smith 2021 "How TikTok Reads Your Mind" The New York Times <u>https://www.nytimes.com/2021/12/05/business/media/tiktok-algorithm.html</u>.

⁶⁴ Id. ("The experience is sometimes described as an addiction ...") See also Allison Zakon 2022 "Optimized for addiction: Extending product liability concepts to defectively designed social media algorithms and overcoming the communications decency act" Wisconsin Law Review (5) <u>https://ssrn.com/abstract=3682048</u>.

⁶⁵ Fairplay 2021 Designing for Disorder <u>https://fairplayforkids.org/pf/designing-disorder/</u>; Tawnell D. Hobbs, Rob Barry, and Yoree Koh 2021 "The Corpse Bride Diet: How TikTok Inundates Teens With Eating-Disorder Videos" *The Wall Street Journal* <u>https://www.wsj.com/articles/how-tiktok-inundates-teens-with-eating-disorder-videos-11639754848</u>; FB Papers titled *Teen Girls Body Image and Social Comparison on Instagram - An Exploratory Study in the US.*

Chase had no history of anxiety or depression, had just made the Olympic Development Program soccer team, had a supportive family, involved parents, and close friends. But TikTok consistently recommended a continuous stream of violent, hopeless, and suicide-themed videos. TikTok selected these videos for Chase even though Chase was searching for things like:

- Bench Press Tips (December 16, 2021)
- Kitchen Hacks (December 29, 2021)
- BoJack Horseman Edits (January 1, 2022)
- Attack on Titan Opening Song (January 9, 2022)
- Trae Young Best Moments (January 28, 2022)
- Motivational Speech (February 5, 2022)
- Gym Motivation (February 10, 2022)

Despite these innocuous searches, Chase's TikTok began connecting and exposing him to male pain, self harm and suicide. TikTok filled Chase's feed with thousands of these videos, which his parents did not know and had no way to find out about. On February 18th, 2022, Chase tragically took his own life, in an uncommon manner strikingly close to a number of videos TikTok identified and sent to him in the weeks prior to his death.

What recommender systems blindly push to children and teens can be extremely disturbing and overtly harmful. For example, one bereaved mother was informed that TikTok was sending other children distressing videos her child posted moments before they took their own life.⁶⁶

A 2021 poll found that 86 percent of parents support rules requiring that automated recommendations be turned off by default. 67

D. <u>Manipulation of Adolescents' Social Anxieties</u>

Parasocial relationships are "one-sided connections" people hold with celebrities, media figures or other characters, and appear particularly important to teenagers and children.⁶⁸ While all people can engage in parasocial relationships (with celebrities etc), children and teenagers have particularly intense and strong parasocial relationships, which are associated with a full range of emotional and personal responses.⁶⁹ The role of parasocial relationships in minors' psychological

⁶⁶ Emily Majewski was 14-years-old when they died by suicide (on December 3, 2021). Emily's last act was to post videos of themself crying and pointing to the closet and belt they planned to use to end their life on TikTok. The police asked TikTok twice to take down Emily's suicide videos (which TikTok continued to amplify and send to other children). TikTok twice refused, stating that the suicide videos were not "explicit enough." A reporter then contacted TikTok about the videos and TikTok's refusal to remove them, and TikTok took them down within a matter of minutes. *See Janet Majewski v. Meta Platforms et al.*, Superior Court of California County of Los Angeles, Case No. 22STCV26829 (filed August 18, 2022) ("Majewski Complaint"), ¶¶ 242-250.

⁶⁷ Accountable Tech 2021 Accountable Tech Frequency Questionnaire 2021 <u>https://accountabletech.org/wp content/uploads/Accountable-Tech-Parents-Poll.pdf</u>.

 ⁶⁸ Tracy Gleason, Sally Theran and Emily Newberg 2017 "Parasocial Interactions and Relationships in Early Adolescence" *Front. Psychol* <u>https://doi.org/10.3389/fpsyg.2017.00</u>.
 ⁶⁹ For example, research shows that in situations of "parasocial relationship break ups," teenagers can be particularly

³⁷ For example, research shows that in situations of "parasocial relationship break ups," teenagers can be particularly affected (Jonathan Cohen 2003 "Parasocial Breakups: Measuring Individual Differences in Responses to the

development can be important. Research has suggested that parasocial relationship formation may help adolescents in particular as they form their own identity and develop autonomy and independence from the family.⁷⁰ Parasocial relationships are common in the digital world, and many apps and websites used by minors include characters which young users are encouraged to develop a parasocial relationship with (such as games that enable you to play "keepy uppy" with Bluey the dog).

However, parasocial relationships developed in the digital world are also often deployed to manipulate minors into extended use and prolonged engagement. Researchers found that 24.8 percent of commonly used children's games exploited parasocial relationships to extend gameplay.⁷¹ This included techniques such as characters expressing disapproval when a child tries to stop playing (for example, with a key character saying "do you want to give up?" when a user decides not to play the next level), pressure in the game narrative (such as having to keep playing to save a main character from violence), or notifications to return to the game (for example, a notification to inform users that "people are protesting in your absence" in a constructed world game).

In many digital products and services, friendship and human connectivity is gamified in ways that drive young people to maximize time and activity on that product. For example, many social media sites display friends or followers counts which creates an implicit drive to "maximize" the number of online friends and followers.

Maximizing the number of online friends is frequently seen as a form of popularity among users,⁷² especially young people. For example, research undertaken for Ofcom, the UK's communications regulator, found that children placed enough value on getting likes and followers on social media that they were prepared to accept people they did not know as friends or followers⁷³, and that this drive for popularity can be quite sophisticated. Children report being concerned not only with their friend count, but their "friends-to-followers" ratio as markers of online popularity.⁷⁴

Dissolution of Parasocial Relationships" Mass Communication and Society,

https://doi.org/10.1207/S15327825MCS0602_5). Further, researchers have explored the full range of emotional responses that can be elicited from parasocial relationships, especially among teens. This ranges from empathy to mood contagion (See Klimmt, Christoph, Tilo Hartmann, and Holger Schramm 2006 "Parasocial interactions and relationships" in Psychology of entertainment, (Mahwah, NJ: Erlbaum) p. 291-313).

⁷⁰ See Tracy Gleason, Sally Theran and Emily Newberg 2017 "Parasocial Interactions and Relationships in Early Adolescence" *Front. Psychol* <u>https://doi.org/10.3389/fpsyg.2017.00</u> and David Giles & John Maltby, 2004 "The role of media figures in adolescent development: relations between autonomy, attachment, and interest in celebrities." *Pers. Individ. Differ.* <u>https://psycnet.apa.org/doi/10.1016/S0191-8869(03)00154-5</u>.

⁷¹ Jenny Radesky, Alexis Hiniker, Caroline McLaren, Eliz Akgun, Alexandria Schaller, Heidi Weeks, Scott Campbell, Ashley Gearhardt 2022 "Prevalence and Characteristics of Manipulative Design in Mobile Applications Used by Children." *JAMA Open Network* <u>https://doi.org/10.1001%2Fjamanetworkopen.2022.17641</u>.

⁷² Stephanie Tom Tong, Brandon Van Der Heide & Lindsey Langwell 2008 "Too Much of a Good Thing? The Relationship Between Number of Friends and Interpersonal Impressions on Facebook" *Journal of Computer Mediated Communication* <u>https://doi.org/10.1111/j.1083-6101.2008.00409.x</u>.

⁷³ For example, "Alice" an 11 year old describes how she was accepting "followers" on Instagram in order to increase her follower count, as it was a mark of popularity among her peers (Ofcom 2016 *Children's Media Lives* <u>https://www.ofcom.org.uk/__data/assets/pdf_file/0015/94002/Childrens-Media-Lives-Year-3-report.pdf.</u> ⁷⁴ Ofcom 2020 *Children's Media Lives* <u>https://www.ofcom.org.uk/__data/assets/pdf_file/0021/190524/cml-year-6-findings.pdf.</u>

The use of social manipulation on social media may uniquely affect young people. As a group of psychologists outlined:

the desire for social acceptance and the fear of social rejection are exploited ... to pull users into social media sites and keep them there for long periods of time. Yet, as psychologists are well aware, children—especially preteens and teens—have particular developmental sensitivities to being socially accepted or rejected.⁷⁵

E. Connecting Young Users to Predatory Adults

In addition to content recommender systems, social media companies are utilizing their sophisticated algorithm products to direct and connect child and teen users with other users (often adults and, all too often, predatory adults) as well as groups, subject matters, and other connections designed to increase engagement. Social media companies have determined that the volume of interactions their users have on their product correlates directly to amount of use and ability to retain users long term.

These algorithms (i.e. user and group recommendations), affirmatively connect minor users to other users and groups based on programming that prioritizes engagement over safety. For example, user recommendation systems identify and direct predators to young children. By some estimates, these systems contribute to the majority of exploitation harms happening to children on these platforms; Meta's own internal research notes these concerns around their friend recommender, or People You May Know (PYMK) feature.⁷⁶ A Meta employee reported findings that "in the past, PYMK [People You May Know] contributed up to 75% of all inappropriate adultminor contact," (that is, grooming). Yet these companies continue utilizing these products in connection with minor accounts, regardless of known harms, because they have likewise determined that connections increase retention.

The consequences of this prioritization can be serious, causing physical harm to children. For example, A.F., an 11 year old, was recommended to dozens of other users, many of whom went on to sexually abuse her (See appendix B:4 and M.F. Complaint).

On October 16, 2021, Instagram user Johnny initiated contact with A.F. and wrote "heyyy." He introduced himself as "houzi from highrise," and asked if this was "another acc you have?" A.F. said yes, she has to "use this one now." He said, "it's fine honey" and told her he only "found [her new account] on accident on my recommended lol." Johnny is one of dozens of adult male Instagram users who found this child on Instagram and then exploited and sexually abused her because Meta directed them to her.

These four examples of acts and practices --rewards, navigational manipulations, content

⁷⁵ ScreenTime Network Our Letter to the APA https://screentimenetwork.org/apa.

⁷⁶ Alexis Spence et al. v. Meta, U.S. District Court for the Northern District of California, Case No. 3:22-cv-03294 (filed June 6, 2022) ("Spence Complaint") p. 11-12, Growth, Friending + PYMK, and Downstream Integrity Problems.

recommender systems and social manipulation — are not mutually exclusive nor exhaustive, but are connected by the deliberate use of psychological insights to drive young people to extend the amount of time they spend on digital products and services.

While extended use designs are "applied through technology, the power to alter behavior is primarily derived from psychology."⁷⁷ The specific use of psychological tactics is morally offensive. A letter from 50 psychologists to the American Psychological Association called on the Association to condemn psychologist's role in extended use design.⁷⁸ It outlined that extended use design

is in opposition to APA Ethical Principles and Standards, including the essential tenet to "take care to do no harm". ... Altering children's behavior without their own or their parents' consent also runs counter to the APA Ethical Principle of Integrity... The great majority of parents have no idea that the social media and video games used by children are developed by psychologists and other experts who use advanced behavior change techniques to pull kids into these platforms and keep them there as long as possible.

Beyond a psychological perspective, from a rights-based perspective deploying these techniques are not in children's best interests; or in other words harmful to their rights. The UN's General Comment on the Rights of Children in Relation to the Digital Environment states outlines how current commercial practices, many of which we have described above "may result in violations or abuses of children's rights, including through advertising design features that anticipate and guide a child's actions towards more extreme content, automated notifications that can interrupt sleep or the use of a child's personal information or location to target potentially harmful commercially driven content."⁷⁹ Extended use designs prioritize commercial best interests.

Many of our young clients and their families report extreme and uncharacteristic reactions when access to social media is limited or prevented which are suggestive of addiction or addictive-like compulsions. This ranges from anger and screaming, to severe depression, to violence, to self-harm to suicide attempts (or in a minority of cases, completed suicide), to running away from home. Our attorneys, and parents, have also observed physical reactions when social media is taken away or even just when a young person considers stopping social media. This includes rapid heartbeat, visible manifestations of anxiety and nervousness, shaking, and similar withdrawal type symptoms. We have had children tell us that if given the choice between stopping their use of

⁷⁷ Richard Freed & Meghan Owenz 2018 "How the Tech Industry Uses Psychology to Hook Children" *Psychology Today* https://www.psychologytoday.com/gb/blog/mental-wealth/201810/how-the-tech-industry-uses-psychologyhook-children.

⁷⁸ ScreenTime Network Our Letter to the APA <u>https://screentimenctwork.org/apa</u>. Similarly, the British Royal College of Psychiatry states that: "young people are particularly vulnerable to compulsive use because they are less able to self-regulate." Royal College of Psychiatrists 2020 Technology use and the mental health of minors CR225. <u>https://www.rcpsych.ac.uk/docs/default-source/improving-care/better-mh-policy/college-reports/college-report-cr225.pdf</u>.

¹⁰ Paragraph 40, United Nations Committee on the Rights of the Child 2021 General comment No. 25 (2021) on children's rights in relation to the digital environment CRC/C/GC/25 <u>https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation</u>.

²¹

social media and losing an arm they would choose loss of an arm because at least they can live without one arm. Many young people tell us that they know that their social media use is harming them, including extreme bullying and sexual abuse that is occuring only through social media. When asked why they don't simply stop logging in, they will say with tears running down their cheeks that they can't stop checking their accounts even though they want to stop, and that they don't know why; that they know that social media hurting them but that they cannot stop and/or feel like they cannot live without it.

At the SMVLC, families routinely report that their child's use of social media harms their relationships, especially when parents try to limit or prevent social media access. This includes family breakdown when children run away or put themselves in harm's way to access social media. For example, one young person lived on the street for months in order to maintain her social media access.⁸⁰ Other clients have run away for hours or days at a time, impacting their education and physical health, exposing them to exploitation and physical harm, and in every case, they talk about being willing to "do it again" if their parents or guardians try to limit or prevent access.⁸¹ But it also creates problems with children as young as 8 and 9 years old, and young people with strong family relationships prior to the start of their social media use. When parents try to prevent or limit social media use, children will engage in all sorts of activities that will produce interfamily conflict. This included lying to their parents (not just to obtain access but also after they have been caught accessing social media), looking for and taking back confiscated devices while their parents. Many young people develop extreme feelings of guilt and shame about this, reflected in journal entries and postings where they say that they have been a burden on their families.⁸²

Lastly, they are fundamentally intrusive. These practices see digital products and services deliberately designed in ways to excessively insert apps, games, websites and other products into young people's lives repeatedly and excessively. The purpose of this *is* to monopolize time and activity. This inherently violates young people's right to be let alone.

III. Behavioral Advertising & Youth Vulnerabilities

Behavioral advertising (or targeted advertising, or personalized advertising) involves tracking and collecting young people's personal data and online activities, and using this information to target them with personalized advertising. Behavioral advertising is common in digital products and

⁸⁰ Amy Neville, et al. v. Snap, Inc., Superior Court of California County of Los Angeles, Case No. 22STCV33500 (filed October 13, 2022) ("Neville et. al. Complaint"), ¶¶ 446-447 (15-year-old dropped out of school and lived on the street for five months in reaction to parental attempts to exert parental oversight and restrict access to the Snapchat product).

⁸¹ See, e.g., <u>Doffing Declaration</u>, ¶ 20-21, 37 ("Whenever I threatened to or did take away her access to social media, she would get angry or violent, or both, and would run away."); *Roy Plunk et al. v. Snap, Inc.*, Superior Court for the State of California for the County of Los Angeles, Case No. 22STCV36229 (filed November 15, 2022) ("<u>Plunk Complain</u>"), ¶ 185 ("... when his parents tried to restrict access, Zach just stopped coming home. He realized that there was literally no way for his parents to prevent him from using Snapchat … and while he was gone, he used Snapchat via friends' devices.").

⁸² See, e.g. <u>Spence Complaint</u> **1**¶ 180 (deception to obtain access), 184 (pits parents against children), 200 (familial conflict as reflected in letter written to Alexis's mom), 207 (Instagram post: "i don't do anything good im a failure im a burden on my family i don't deserve to exist").

²²

services that minors use, and that are targeted at children. For example, a study of children's specific apps found that 95 percent included at least one form of advertising,⁸³ and eight of the most popular apps used daily by minors (aged 9-17) include targeted ads, and the other two are owned by large vertically integrated tech companies who use their data to enable targeting (Meta and Google).⁸⁴

As this suggests behavioral advertising requires masses of personal data; it is fueled by data hungry machine learning AI models.⁸⁵ Like the advertising itself, collecting and transferring minors 's data for advertising is rife:

- One investigation found that two-thirds of apps played by preschool-aged children collected and shared personal data⁸⁶ (persistent digital identifiers, which are used to link-IDs in advertising profiles).
- Another analysis of 959,000 apps on the Google play store in the UK and US found that apps targeting children had the highest number of third-party tracker apps collecting and transferring data to other companies⁸⁷ (largely a process done for behavioral advertising).
- An analysis of 5,855 popular free children's apps found that many collected personal information such as geolocation data, contact data, unique phone identifiers, and the majority violated COPPA because they use third party Software Development Kits (SDKs) that collect and enable transfer of children's data⁸⁸ (again, a process largely done for advertising).
- A study of EdTech products used in Texan and Californian schools found that EdTech apps and products recommended to school children during the pandemic included cookies, tracking pixels and SDKs that enable data collection and transfer (again, largely for advertising purposes).⁸⁹

⁸³Marisa Meyer, Victoria Adkins, Nalingna Yuan, Heidi Weeks, Yung-Ju Chang & Jenny Radesky 2019 "Advertising in Young Children's Apps: A Content Analysis." *Journal of Developmental & Behavioral Pediatrics:* https://pubmed.ncbi.nlm.nih.gov/30371646/#:~:text=DOI%3A-,10.1097/DBP,00000000000622,-Full%20text%20links.

⁸⁴ According to a study of 2,002 young people conducted by Thorn and Benenson Strategy Group they are; YouTube, Instagram, Snapchat, TikTok, Facebook, Google Hangouts/Meet, Messenger, Twitter, WhatsApp, Among Us. (See Thorn 2021 Responding to Online Threats: Minors Perspectives of Disclosing, Reporting & Blocking <u>http://info.thorn.org/hubfs/Research/Responding%20to%20Online%20Threats_2021-Full-Report.pdf</u>).
⁸⁵ For example, Google claims to have put these powerful AI models into the hands of every advertiser (See Jerry

²⁵ For example, Google claims to have put these powerful AI models into the hands of every advertiser (See Jerry Dischler 2018 "Putting machine learning into the hands of every advertiser" Google: The Keyword <a href="https://www.downwarefunctions.com/google.

https://support.google.com/google-ads/answer/9065075?hl=en-GB). ⁸⁶ Fangwei Zhao, Serge Egelman, Heide Weeks, Nico Kaciroti, Alison Miller & Jenny Radesky 2020 "Data Collection Practices of Mobile Applications Played by Preschool-Aged Children." *JAMA Pediatr.* https://jamanetwork.com/journals/jamapediatrics/fullarticle/2769689.

⁸⁷ Reuben Binns, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert, Nigel Shadbolt 2018 "Third Party Tracking in the Mobile Ecosystem" In WebSci '18: 10th ACM Conference on Web Science <u>https://doi.org/10.1145/3201064.3201089.</u>

 ⁸⁸ Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman 2018 "Won't Somebody Think of the Children?" *Proceedings on Privacy Enhancing Technologies* <u>https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf</u>.
 ⁸⁹ Human Rights Watch 2022 *How Dare They Peep into My Private Life*

https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments.

²³

While studies of the impact of behavioral advertising on minors are limited, evidence suggests that they are highly susceptible to it. Research has shown that higher levels of targeting involving more personalized use of data generate stronger responses in teens regardless of their concerns about privacy⁹⁰ — i.e. they are unable to turn their concerns about their privacy into effective safeguarding strategies from this advertising. Other research has shown that when textual "debriefing" is provided initially high purchase intentions decrease —⁹¹ i.e. when teenagers are provided with more information about the mechanics of the practice, they moderate their intentions accordingly. This vulnerability is more pronounced for younger children. Experimental research has how they are not driven to higher purchase intentions because they experience targeted ads as more relevant, but because targeted ads affect how much children "like" being advertised to *because they do not recognize they are being targeted*. The researchers conclude "thus, children seem to process targeted online advertising in a noncritical manner"⁹² vis a vis adults.

329

Behavioral advertising, and the collection and use of all of this data to fuel it, is not a practice that meets community expectations. A 2021 poll found that 88 percent of parents support banning the practice of tracking and targeting kids and teens with ads based on their behavioral profiles.⁹³ Likewise, academic research has shown that parents are highly concerned about teenager's exposure to personalized advertising and underpinning online data collection practices, reporting significantly more negative downsides than positive aspects.⁹⁴

Internal research from Instagram reveals that young people may be unhappy with it as well. Teens identify "inappropriate advertisements targeted to vulnerable groups" as one way in which "Instagram harms their mental health" and that "Teens called out ad targeting on Instagram as feeding insecurities, especially around weight and body image."⁹⁵ Moreover, teens want to be able to "opt out of advertising categories that are personally triggering, such as skinny teas and lollipops or waist-trainers."⁹⁶ Behavioral advertising is a product feature young people have asked Instagram to turn off. This would provide young users with some actual control over their social media

⁹⁰ Michel Walrave, Karolien Poels, Marjolijn L. Antheunis, Evert Van den Broeck & Guda van Noort 2018 "Like or dislike? Adolescents' responses to personalized social network site advertising," *Journal of Marketing Communications*, <u>https://doi.org/10.1080/13527266.2016.1182938</u>.

⁹¹ Brahim Zarouali , Koen Ponnet, Michel Walrave, Karolien Poels 2017 ""Do you like cookies?" Adolescents' skeptical processing of retargeted Facebook-ads and the moderating role of privacy concern and a textual debriefing" *Computers in Human Behavior* <u>http://dx.doi.org/10.1016/j.chb.2016.11.050</u>.

⁹² Eva A, van Reijmersdal, Esther Rozendaal, Nadia Smink, Guda van Noort & Moniek Buijzen 2017 "Processes and effects of targeted online advertising among children" *International Journal of Advertising <u>https://doi-org.ezproxy-b.deakin.edu.au/10.1080/02650487.2016.1196904</u>.*

⁹³ Accountable Tech 2021 Accountable Tech Frequency Questionnaire 2021 <u>https://accountabletech.org/wpcontent/uploads/Accountable-Tech-Parents-Poll.pdf</u>.

⁹⁴ Sanne Holvoet, Liselot Hudders, Laura Herrewijn 2021 "How to empower parental responsibility: parents' views on personalized advertising and online data collection targeting their teens" *Young Consumer* <u>ISSN: 1747-3616</u>.
⁹⁵ Teen Mental Health Deep Dive, p. 28, 39, Published by The Wall Street Journal September 29, 2021,

https://digitalwellbeing.org/wp-content/uploads/2021/10/Facebook-Files-Teen-Mental-Health-Deep-Dive.pdf. 96 Id. at p. 54.

²⁴

experience,⁹⁷ but at the expense of advertising revenue to social media companies - which is presumably why these companies have not implemented such product changes.

Given the widespread disapproval, the mechanics of the practice often happen "in the dark." There is often no process for consumers to give or deny permission for this, and research has shown that consumers have little knowledge about how this practice affects and operates on them.⁹⁸ For example, consumers may be unaware that their ISP is logging their browsing history to build profiles for behavioral advertising.99 Many companies rely, ethically and legally where required, on problematic notice and consent processes and complex privacy policies to justify processing consumer's data for behavioral advertising. The problems of privacy policies are well known, but these extend to products frequently used by minors . A study of the privacy policies of 10 popular apps and products used by young people found that nine of them required a college level degree to understand and on average they each take one hour and 45 minutes to read.¹⁰⁰

This lack of awareness is demonstrable: research has shown that American parents have, at best, only a moderate understanding of common online marketing tactics deployed in children's apps and products.¹⁰¹ Likewise, research has found that advertising literacy and awareness of commercial data practices is limited among children but only begins to evolve to "adult like" levels at the age of 16.102 Neither parents, children nor teens appear particularly equipped to make informed choices when it comes to behavioral advertising.

Frequently, this darkness becomes active obfuscation. Research into privacy policies and procedures used by 10 apps popular with young people noted that eight out of ten deployed dark patterns regarding data and privacy policies, which actively attempted to "trick" young people into agreeing to sharing more personal data than is necessary.¹⁰³ Dark patterns are frequently deployed in children's apps too, which encourage users to share more information than is necessary. For example, minors' games often ask young people to share their location or phone books, or encourage them to "share their top score," which requires linking the app to social media

⁹⁷ See 47 U.S. Code Section 230 - Protection for private blocking and screening of offensive material. A fundamental congressional finding in support of Section 230 is the "great degree of control" interactive computer service providers give to users "over the information that they receive." These companies seek to hide behind the protections of Section 230, but have designed their products in a way such that the companies themselves exert nearcomplete control over the user experience, subverting the very purpose of Section 230 in a manner that is deceptive and unfair to consumers.

¹⁸ See Chang-Dae Ham 2017 "Exploring how consumers cope with online behavioral advertising," International Journal of Advertising, https://doi.org/10.1080/02650487.2016.1239878

⁹⁹ See FTC 2021 A Look At What ISPs Know About You: Examining The Privacy Practices Of Six Major Internet Service Providers | Staff Report https://www.ftc.gov/reports/look-what-isps-know-about-you-examining-privacypractices-six-major-internet-service-providers.

Reset 2021 Did We Really Consent to This?

https://au.reset.tech/uploads/l01_resettechaustralia_policymemo_t_c_report_final-july.pdf.

Matthew A. Lapierre, Eunjoo Choi 2021 "Parental awareness of new online advertising techniques targeting children: an exploratory study of American parents" Young Consumers ISSN: 1747-3616.

Brahim Zarouali, Valerie Verdoodt, Michel Walrave, Karolien Poels, Koen Ponnet, Eva Lievens 2020 "Adolescents' advertising literacy and privacy protection strategies in the context of targeted advertising on social networking sites: implications for regulation" Young Consumers <u>ISSN: 1747-3616</u>. ¹⁰³ Reset 2021 Did We Really Consent to This?

https://au.reset.tech/uploads/l01_resettechaustralia_policymemo_t_c_report_final-july.pdf.

²⁵

accounts.¹⁰⁴ It is not always explicitly clear that this will allow additional data collection and transfer.

Given that parents and teens disapprove of the practice, it is unclear whether they would continue to use the same digital service and products, or use them in the same way, if the use of personal data for behavioral advertising was more accurately represented to them. This makes behavioral advertising deceptive when deployed on minors. The lack of accessible and clear information provided to minors, and their parents, is a material representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances.¹⁰⁵

Deception is inherently harmful because it deprives consumers of the ability to make free and informed choices about products and services. This is why the FTC need not show harm to consumers in order to demonstrate unlawful deception under Section 5 of the FTC act;

A representation, omission, or practice is deceptive under Section 5 if it is likely to mislead consumers acting reasonably under the circumstances and is material to consumers—that is, it would likely affect the consumer's conduct or decision with regard to a product or service.

Behavioral advertising is also manipulative when deployed on minors. Manipulation involves the use of commercial surveillance practices to covertly exploit minor users' cognitive and emotional vulnerabilities and deprive them of autonomy. Socila media companies that engage in these practices are able to effectively take control of the minor consumer's decision-making process and cause them to act in the best interests of the surveillance company. There are three important components of manipulative practices:¹⁰⁶

- A. The exploitation of an minors' vulnerabilities;
- B. The use of covertness as a tactic, and;
- C. Divergence of interests between the surveillance company and the target consumer.

Behavioral advertising, when deployed on minors, demonstrates all three components. First, it deliberately attempts to exploit the individual vulnerabilities of minors. This exploitation is "baked into" the process, where personal data (including personal sensitive data) is processed and used to deliberately serve young people the ads they will be most likely to succumb to. This is more than just a commercial and economic threat to young people – and companies often appear to enable the explicit targeting of "risky" vulnerabilities. For example, Facebook was caught bragging to advertisers about their ability to target young people when they were feeling

¹⁰⁴ Science Daily 2018 "Advertising in kids' apps more prevalent than parents may realize" https://www.sciencedaily.com/releases/2018/10/181030091452.htm.

 ¹⁰⁵ FTC 1983 FTC Policy Statement on Deception <u>https://www.ftc.gov/legal-library/browse/ftc-policy-statement-deception</u>.
 ¹⁰⁶ See Daniel Susser, Beate Roessler, & Helen Nissenbaum 2019 "Technology, autonomy, and manipulation"

¹⁰⁶ See Daniel Susser, Beate Roessler, & Helen Nissenbaum 2019 "Technology, autonomy, and manipulation" Internet Policy Review, <u>https://doi.org/10.14763/2019.2.1410</u>.

²⁶

"insecure," "worthless," and "need a confidence boost."¹⁰⁷ Research has shown that Facebook does not exercise care nor caution with this invasive, "risky" targeting. Researchers tested their system and demonstrated that Facebook would allow advertisements that promoted "Cocktail recipes from what you can steal in your parents liquor cabinet" to young people Facebook identified as interested in alcohol, weight loss offers to young women interested in extreme weight loss,¹⁰⁸ or drug-fuelled skittles party to teenagers interested in pharmaceuticals.¹⁰⁹

This demonstrates significant divergence of interest between the company and the consumer; it is never in a young person's best interest to target them with a drug or alcohol ad, but especially if they may be vulnerable to drug and alcohol abuse.

This is also a deeply covert tactic. On top of the deceptive nature of the practice as described above, companies appear to go out of their way to "hide" the fact that they use minors' personal data to target them for behavioral advertising. For example, after the research demonstrating "risky" targeting was released, Facebook later claimed to have turned off the ability for advertisers to target teenagers interested in drugs, alcohol and gambling – at a US Senate hearing no less.¹¹⁰ However, subsequent research has shown that Facebook's advertising recommender algorithm will still place any "risky" ads they approve into the feeds of young people who are the most vulnerable to them. In all likelihood, the research concluded, the ability to target vulnerable teens would be worse.¹¹¹ Or as France Haugen put it, when asked about Facebook's claim to have turned off the ability to target vulnerable teens with ads for "partying" content:

I'm very suspicious that personalized ads are still not being delivered to teenagers on Instagram because the algorithms learn correlations. They learn interactions where your party ad may still go to kids interested in partying because Facebook almost certainly has a ranking model in the background that says this person wants more party-related content.¹¹²

As a deceptive and manipulative practice, behavioral advertising inherently harms minors 's autonomy. But it also drives masses of inappropriate data security, which generates a range of

 ¹⁰⁷ See Darren Davidson 2017 "Facebook targets 'insecure' young people" The Australian <u>https://theaustralian.com.au/business/media/digital/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6</u>.
 ¹⁰⁸ Reset 2021 Profiling Children for Advertising: Facebook's Monetisation of Young People's Personal Data

¹⁰⁸ Reset 2021 Profiling Children for Advertising: Facebook's Monetisation of Young People's Personal Data <u>https://au.reset.tech/uploads/resettechaustralia_profiling-children-for-advertising-1.pdf</u>.

¹⁰⁹ Tech Transparency Project 2021 Pills, Cocktails, and Anorexia: Facebook Allows Harmful Ads to Target Teens <u>https://www.techtransparencyproject.org/articles/pills-cocktails-and-anorexia-facebook-allows-harmful-ads-target-teens</u>.

teens. ¹¹⁰ Facebook now only allow advertisers to actively select young people based on only allow advertisers to target ads to people under 18 based on their age, gender and location, according to testimony from Facebook's head of safety to the Senate Subcommittee on Consumer Protection's inquiry into, *Product Safety, and Data Security on Facebook and Instagram's impact on teens, 9/30/2021.*

 ¹¹¹ Natasha Lomas 2021 "Facebook accused of continuing to surveil teens for ad targeting" *TechCrunch* <u>https://techcrunch.com/2021/11/16/facebook-accused-of-still-targeting-teens-with-ads/</u>.
 ¹¹² France's Haugen to Senate Subcommittee on Consumer Protection's inquiry into, *Product Safety, and Data*

¹¹² France's Haugen to Senate Subcommittee on Consumer Protection's inquiry into, *Product Safety, and Data Security on Facebook and Instagram's impact on teens*, 10/5/2021.

other cognizable harms, from fueling the data breaches enabling identity theft¹¹³ to entrenching discrimination.114

Conclusion

When deployed on minors, extended use design and behavioral advertising is unreasonably dangerous. The nature and extent of these practices is not disclosed to minor users or their parents and is likely to cause substantial injury to kids. These practices deliberately push young people towards overuse, problematic use and addiction. As established by the examples and cases describe above, the nature of harms minors suffer are diverse and often serious, including death and sexual exploitation, and these companies know that their products are causing these harms.

Meta's own estimates put problematic use of their products at least 12.5 percent across all users, and estimates that the use of its product makes thoughts of suicide and self-harm worse in 13.5 percent of teen girl users and body image issues worse in 33 percent of teen girl users.¹¹⁵ At the same time, most American teens use these products regularly, if not compulsively and every day: Instagram (62 percent), Snapchat (59 percent), and TikTok (67 percent).¹¹⁶ All of this equates to millions of U.S. children and teens being exposed to substantial and widespread harms every single day, for the sole benefit of the social media companies creating (though not disclosing) these consumer safety risks. There are very limited countervailing benefits to consumers and no countervailing benefits to competition. On the contrary, the largest social media companies have obtained a near-monopoly through their "teen lock-in" techniques, making it impossible for other companies - particularly those seeking to implement consumer and child safety practices - to compete.

Parents, young people and children often have limited understanding about the mechanics of these products and practices. The products are deliberately designed this way; for example, as Appendix B:5 highlights, even technologically sophisticated parents, experienced web developers, are unable to navigate Meta's reporting systems as currently designed. Parents and young people are actively misled with material misrepresentations and marketing strategies designed to convince consumers that these products are non-addictive, fun, and safe for kids when we know that the opposite is true

¹¹³ In 2021, 1 in 45 American children had personal information that was exposed in a data breach and 1 in 50 were victims of ID fraud. This can cause severe economic harms; the average family loses in excess of \$1,000 when a child falls victim to identity fraud. In 2021 alone, fraud losses linked to child identity fraud totaled \$918 million, averaging \$737 per family (Tracev Kitten 2021, Child Identity Fraud https://javelinstrategy.com/research/childidentity-fraud-web-deception-and-loss). ¹¹⁴ For example, schools serving primarily students of color are more likely to use intensive surveillance

technologies and collect unnecessary data than other schools (Jason Nance 2017 'Student Surveillance, Racial Inequalities, and Implicit Racial Bias', Emory Law Journal https://scholarlycommons.law.emory.edu/elj/vol66/iss4/1).

Georgia Wells, Jeff Horwitz & Deepa Seetharaman 2021 "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show" Wall Street Journal https://www.wsj.com/articles/facebook-knows-instagram-is-toxicfor-teen-girls-company-documents-show-11631620739.

https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/.

I urge this Committee to draft and report bipartisan legislation to provide parents, educators, community leaders, health professionals and government regulators with the legal tools to address the carnage that social media is inflicting on America's youth. Social media companies should be held to the same standard of accountability as any other business for the harms they knowingly inflict on vulnerable kids. Parents of all political persuasions, cultural backgrounds and geographic regions who every day confront the malign effects of social media on their kids are crying out "enough is enough." Congress must act now to protect our kids and safeguard our future.

[This page is intentionally left blank.]

Appendix A: PERSONAL NARRATIVES FROM YOUNG PEOPLE

1. Emi's story,¹¹⁷ highlighting the impact of push notifications

My name is Emily "Emi" Kim, and I am an 18-year-old from Los Angeles, California. I want to tell you about my experience with social media and how that experience pushed me to fight for much-needed change -- I want to talk about my story and how tech platforms could and should have stepped up to prevent many of the issues that I experienced.

... I got my first cell phone at the end of sixth grade, I would have been 12 turning 13. My older brother and I went to different schools. After school, I would wait for my brother to pick me up. My new cell phone was the perfect way for my entire family to keep in touch; my brother could tell me he was running late, and my mother could reach out to find out where I was. It was a great tool, but it came at a high cost.

Most of my classmates had already had years of experience using platforms like Instagram and Snapchat. My peers would have been under 13, some even 11, when they started with these platforms — it's difficult to imagine that these platforms do not know 11 year olds are using their services. These platforms are not built for 11 year olds, and yet there my peers were. Something was bound to go wrong.

... There's no clear understanding about what social media is when you join up, it felt like a game. It felt like a social game, with "like" numbers and social numbers, and when something goes wrong you think you are misunderstanding the game or playing the game wrong. You don't think about the company that made the game. And in this game, it was not clear to me what to do when something went wrong.

... My online torment started up again later in middle school when I was diagnosed with alopecia areata, an autoimmune disorder that leads to significant hair loss. Female classmates would post photos of themselves lying on the floor with their hair twisted to look like hearts — a trend I could not participate in. Although I know that the trend originated from Kendall Jenner, and the photos kids were uploading weren't aimed at me, nevertheless, I felt targeted. I was not open about my alopecia at that time.

... The longer I scrolled on Instagram or watched Snapchat Stories, the more I'd see "Instagram girls" from my school — the lucky ones who could choose how exactly they wanted their hair to look and had the long, flowing hair to do it. I kept logging in because I wanted to fit in, and on social media it felt like it was possible to fit in, if you got enough likes you could be successful and popular. So I kept logging in, I couldn't help but want to be successful and popular. But this was also the time that Instagram stories came out, and when someone uploaded a new story there would be a push notification. And I'd get this notification that one of my classmates or one of my

¹¹⁷ Also published in Emi Kim 2021 "Social media reforms can ease negative impact on CA youth" Sacramento Bee <u>https://www.sacbee.com/opinion/op-ed/article260522907.html</u>.

friends had a new story. I'd click on the notification and get sent yet another story that made me feel like I couldn't fit in. I'd see all of these pictures of girls with perfect hair and ponytails and buns. I'd like these pictures, I'd comment on them, because I felt like I had to. And then because I interacted with that post, I'd get more recommendations for those sorts of posts. So I got more notifications.

Despite not posting photos of myself, I still felt horrible whenever I was on a social media platform, but I started feeling excluded from conversations at school. I was measuring myself up to all of my peers on these platforms and I felt like I was losing. I now know that platforms are designed to encourage young people to compare and measure themselves up — "social comparison" — and they know it harms people, like it did me. It makes me feel disposable, as if I am not welcome and not needed, and to think that this is a design feature of these platforms is shocking.

2. Kelsey's story,¹¹⁸ highlighting the impact of content recommender systems

I am a 17-year-old high school student in Southern California, and I am an eating disordersurvivor-turned-activist. I've struggled with disordered eating and body image since I was 6 years old when I started school. Social media plays a significant role in my struggle.

Social media platforms flood kids with connections and subject matters that seem to promote and normalize eating disorders or using unhealthy methods to lose weight. For example, every day on Instagram and Tik Tok there are new viral trends that promote ingesting weight loss supplements or diet products which are supposed to "help you get your dream body". It is not just that these exist on Instagram but that Instagram has decided that this is what school-age kids want to see so it targets them with never-ending loops filled with these sorts of harms. School-age students who see these types of "quick fix" weight loss or body image solutions, can be easily fooled into believing and trying these dangerous trends — sometimes with dangerous or deadly consequences.

This is the sort of content that used to fill my Instagram feed. As someone who had grown up with Instagram, I can't recall a time when the app <u>didn't</u> show me this sort of dangerous content. I felt like Instagram's and its algorithms were always populating my feed with it, almost from the moment I created my account.

At one point, it got so normalized that prominent figures like the Kardashians were openly promoting weight loss supplements and diet suppressors. I hadn't had an interest in these things and yet they'd pop up on my screen like magic.

Having achieved recovery from an eating disorder and currently actively working to better my relationship with my body, I can say that at this point whenever Instagram or Tiktok recommends this kind of content, I immediately block it from my feed so Instagram's algorithm learns not to show me this kind of material again. I have moved on. I have to take active steps to stop the platform from recommending this content. Without my consent, Instagram pushes me towards it, but I have to pull myself away from it.

But that wasn't possible for me 2 years ago. At the height of my eating disorder, I used social media as a fuel for my obsession with weight loss. I took the images they recommended of perfectly toned bodies and tips for weight loss religiously. When I was at my worst, this kind of content on my Instagram feed motivated me to continue down an unhealthy path. When I finally decided enough was enough, I knew I couldn't rely on Instagram to send me the positive messages I needed, I had to actively try and change my social media feeds, I had to do the hard work. This content was just always in my feed already, and somehow it was *my* responsibility to get it out.

And I know I'm not alone. Generation Z holds the unwanted record of having some of the highest rates of suicide and mental health issues. We feel more stressed, anxious, and lonely than any other

¹¹⁸ Also published in Kelsey Wu 2021 "Body Image and Social Media" KQED

https://www.kqed.org/perspectives/201601142393/kelsey-wu-body-image-and-social-media.

generation. I feel that much of this truly is due to the algorithmic recommendations and content pushed on us by social media platforms.

Appendix B: SUMMARIES OF FILED LAWSUIT EXAMPLES

1: Suicide, self harm & addiction cases

A. Brantley Aranda (Louisiana), December 30, 2001-September 4, 2019.119

Brantley was 17 when he died.

Brantley's mother could not keep him off social media as he had access to the internet while at school. In an attempt to protect him, she allowed him to open a single Facebook account in May of 2018, when he was 16-years-old. At that time, he could not get Facebook on his cell phone, so had to access it via the family computer with supervision and time limits.

In May of 2019, Brantley got a new phone and immediately began receiving Facebook's push notifications - designed to keep him on the app - at all hours of the day and night. Brantley began accessing Facebook every chance he got, to the point where he no longer slept. Facebook began recommending other users with whom he should connect, and decided which subject matters he should view. Brantley once commented to his mother that after he and his girlfriend broke up he started receiving relationship advice and romance-themed content from Facebook, which he did not want and which made him sad; but that he did know how to get Facebook to stop.

Shortly after Brantley gained access to Facebook on his cell phone he began staying awake until 3 and 4 am engaged with the Facebook product. Meta tracks all usage and was aware of Brantley's excessive and dangerous use of its product, while his own parents were not - and had no way to ascertain such problematic use since Brantley appeared to be sleeping whenever his mother passed by his room. As a result of Facebook's engineered addiction, Brantley began to suffer from severe sleep deprivation and anxiety so extreme that it manifested in physical symptoms like shortness of breath and chest pain. His parents became concerned that he might have a heart condition so took him to the doctor for testing, but doctors found nothing wrong other than orthostatic hypertension.

On Wednesday, September 4, 2019 - less than four months after Brantley got his first cell phone device capable of accessing Facebook - he got into a fight with his brother and his father took away his phone as a consequence for that behavior. The family attended Wednesday night church and Brantley headed home after church with his grandparents while his parents stayed to help cook food. Brantley told his grandparents he had homework so headed home and when his mother returned from church that night she found her son with a bullet in his chest, and a note that read "I'm sorry for everything."

B. Emma Claire Gill (Louisiana), September 2, 2004-August 8, 2021.120

35

¹¹⁹ Blair Aranda et al. v. Meta Platforms, Inc., District Court for the Northern District of California, Case No. 3:22-cv-04209 (filed July 20, 2022) ("<u>Aranda Complaint</u>").

¹²⁰ Darla Gill, et al. v. Meta Platforms, Inc. et al., District Court for the Western District of Louisiana, Case No. 1:22-cv-O2173 (filed July 20, 2022) ("<u>Gill Complaint</u>").

Emma Claire was 16 when she died.

Emma Claire got her first cell phone in 2015 when she was 10. She was staying late after school and her parents wanted her to have a way to reach them. The device was pre-paid with limited minutes, such that her parents did not believe that she could access social media. Nor did they have any knowledge of any accounts until sometime in 2016 or 2017, which is when a family member told them that she had an Instagram. Emma Claire's parents did not consent, but Meta did not require their consent and they had no means to prevent her from using Instagram. Instagram then targeted Emma Claire with subject matters and advertising that had a foreseeable and harmful impact on her self-image and self-esteem, resulting in some anxiety and difficulty with focus. In June of 2020, Emma Claire's mother took her to a counselor, who referred to Emma Claire as a "well adjusted normal 15 year old." Meta tracks usage, and had full knowledge as to both the subject matters it was directing to Emma Claire and any excessive and other harmful use. For her parents and counselor, however, there were no signs, reporting, or red flags to follow so that they could identify and help Emma Claire with the issues social media was causing.

At some point, Emma Claire's parents learned that she had opened a TikTok account against their express prohibition. As with Instagram, however, the TikTok product is designed in a manner that gives parents no actual control or say in whether their children can use it. Then, in August of 2020, Emma Claire asked her parents to allow her to open a Snapchat account. Her school and sports team communicated via Snapchat and Emma Claire promised to close her TikTok account as well as a secondary Instagram account she had opened without their knowledge if she could open a Snapchat. Emma Claire's parents understood that Snapchat was a silly photo app, used by Emma Claire's sports team and teachers, and marketed to children - so they agreed.

On August 15, 2020, Emma Claire opened her first Snapchat account. She quickly became addicted to the Snapchat product, including Snap's hidden rewards and Snapstreaks. She was then exposed and connected to other users who bullied and abused her (through Snapchat's Quick Add feature and its direct messaging and accessibility features as applied to minor accounts). She also was convinced to send explicit photos via Snapchat based on her belief in Snap's marketing - which assures minors that their photos disappear.

On August 7, 2021, Emma Claire snuck out with her best friend to meet up with a boy. Her mother caught her sneaking back into the house, and took her phone as a consequence. This was not an angry situation, but rather, her mom went through Emma Claire's phone and talked with her about what she found. She held her daughter until Emma Claire fell back asleep. The next morning, while her parents got ready for church, Emma Claire went to feed the pigs. Instead, she grabbed her father's gun from his truck and shot herself in the barn.

2: Social comparison & eating disorder harms

In the case of disordered eating content, we have found that certain social media companies - predominantly Meta and TikTok, though there may be others - are targeting children and young girls disproportionately with social comparison, body image, self-harm, and disordered eating content. These types of harms originate with the social media company. For example, most children and teens do not search for or request disordered eating content¹²¹; they are introduced to these subject matters by the social media companies' programming decisions; and over time, as the algorithms determine that such overtly harmful connections, user and group recommendations, and content are increasing engagement, they begin flooding the user experience with little else. These programming and engagement mechanisms are even more dangerous to minor users when coupled with product practices and features such as, failure to verify age and parental consent, continued distribution absent such consent, public profile and direct messaging accessibility settings and defaults routinely applied to minor accounts, and the sheer volume of recommendations, connections, and advertisements aimed at minor users.

<u>A. Alexis Spence, et al. v. Meta Platforms Inc.</u>, District Court for the Northern District of California, Case No. 3:22-cv-03294 (filed June 6, 2022).

Alexis Spence was 11 when she opened her first Instagram account, without her parents' knowledge or consent. She used friends' devices, as well as an Ipod device, which was marketed and used for music such that her parents did not know it had wi-fi access. She began using Instagram because she was interested in Webkinz (interactive stuffed animals) and wanted to follow Webkinz pages. She frequently posted her real age in public comments, as well as her public profile which announced that she was eleven and then twelve years old. She also eventually learned from Instagram videos how to bypass various parental control programs and software her parents had installed on those devices where they knew she could access social media.

Alexis quickly became addicted to the Instagram product, and began sneaking around and lying to her parents so that she could continue using it. In December of 2014, when Alexis was 12, she got her first smartphone and learned from other Instagram users how to bypass the parental control software her parents installed; her parents also required all devices to be left in the hall at night, but Alexis began sneaking out to get her phone after her parents fell asleep. Alexis suffered severe sleep deprivation as a result. And the more time she spent on Instagram, the more Meta's code began escalating her user experience in the interest of prioritizing engagement over user safety. Meta's programming began sending 12-year-old Alexis massive amounts of social comparison and disordered eating content, and within four months of gaining this increased access to Instagram Alexis's entire self-image was destroyed. In April of 2015, Alexis drew this disturbing self-portrait (the first of its kind),

¹²¹ Most of the children with whom we work were taken down this rabbit hold by social media companies after looking for delicious recipes (*see, e.g.* <u>Wuest Complaint</u>, ¶¶ 174-176, <u>J.S. Complaint</u>, ¶ 210), or fitness content to help them combat the stagnancy caused by the pandemic.



For years, Meta continued to flood Alexis's Explore page with thigh gaps and models skinny to the point of illness. Meta likewise directed "health and beauty" advertisements to her, recommended and connected her with other (often adult) users and influencers suffering from disordered eating, and directed her to groups and group members who encouraged Alexis in her eating disorder and self-harm, and told her to hide it from her parents. One of the product features Alexis recalls was the live, group chat feature, where adults could invite minors and would encourage Alexis and others in these harmful behaviors. Alexis' parents did not know that Alexis was on Instagram and when they eventually caught her (years later) they still did not know about her secondary accounts, about Meta's direct message features, group and user recommendations, or the multitude of other, harmful products Meta distributes to kids but does not advertise or disclose to parents. Jeff and Kathleen Spence were completely in the dark while Meta was harming their child.

Alexis wanted to find a place to belong and believed that she could not live without Instagram, but then she also felt worse about herself and more anxious and depressed every time she used Instagram. In February 2016, Meta quietly rolled out a product feature that enabled users to switch easily between accounts - this refers to a FINSTA, which is a secondary account, often opened by teen users and hidden from family and/or friends. This product feature (unknown to most parents and not openly disclosed by Meta) made it easier for children to hide their use of multiple accounts. As intended, Alexis opened several new FINSTAs as soon as Meta's new feature rolled out, which made it even harder for her parents to find out what was happening. When they asked about accounts, Alexis denied that she had any. In May of 2018, one of Alexis' friends reported to the school that they were concerned Alexis might harm or even kill herself, based on posts Alexis made to one or more of her FINSTAs. Alexis was hospitalized and diagnosed with Anorexia Nervosa and associated habits of purging, as well as major depressive disorder and anxiety. It was only when Alexis had no access to social media, in treatment, that she began to feel better. Her road to recovery was long and Alexis still struggles, and will struggle for the rest of her life.

B. D.S. et al. v. TikTok Inc and ByteDance Inc., Los Angeles County Superior Court, Case No. 22STCV24332 (filed July 28, 2022).

K.S. got her first cell phone at 10 as she was taking the bus home from school alone for the first time and her parents wanted her to have a way to reach them. Around when the pandemic started, K.S. opened her first TikTok account, without her parents' knowledge or consent. Her use escalated during periods of remote learning, when it was difficult for her parents - both working - to monitor her around the clock. K.S. gradually began to change from a gregarious and outgoing kid to someone who was quiet and withdrawn. Her parents artibuted it to the pandemic at first, but when K.S. went back to in-person school in August of 2020 things did not improve. K.S. had always been athletic and interested in sports, and TikTok's recommendation technologies took this interest and decided to send her massive amounts of disordered eating themed videos. TikTok pushed more and more how-to videos to K.S. about how to lose weight in extreme ways, encouraging her to limit her caloric intake and inundating her with content about how she should be skinny at any cost.

K.S. parents were regularly checking her phone, and eventually found out about TikTok. They tried to delete the app, but when the phone backed up it would reappear. They did not know how to keep TikTok away from their child, and TikTok did not provide them with a 1-800 number or any resources or tutorial for how to accomplish that. K.S.'s mother also tried checking TikTok and K.S.'s phone in general, to see if she could find out what was happening to her child. But she did not have a TikTok and did not know how to use the product, so only saw the "Favorites" page - the product feature that shows pages and content a user has chosen to follow - which contained sports themed videos.

In December of 2021, K.S.'s grandfather told her mother about an article in The Wall Street Journal titled "The Corpse Bride Diet': How TikTok Inundates Teens With Eating-Disorder Videos." Her mother checked her TikTok, and knew this time to check the "For You" page, which is how she learned that TikTok was inundating her daughter with exceptionally disturbing content. TikTok was destroying K.S.'s self-confidence and sense of self, and K.S. was not yet even 13 years old. TikTok knew that K.S. was a child and programmed its recommendation algorithms to send her inherently harmful and extreme subject matters anyway.

K.S. currently is 13 and in recovery, and no longer uses the TikTok product.

We have a number of cases similar to the fact patterns in the <u>Spence</u> and <u>K.S.</u> cases, but where the minors at issue have been unable to stop using the social media products that are harming them. In those instances, our clients are not in recovery or are struggling to stay in recovery while they continue to suffer the harms these products cause. Examples include,

 <u>I.J. et al v. Meta Platforms Inc.</u>, TikTok Inc, and ByteDance Inc., Los Angeles County Superior Court, Case No. 22STCV28201 (filed August 30, 2022). A.D. was 12 when she opened her first Instagram and TikTok accounts (without parental knowledge or consent) and is currently 16. TikTok and Meta advertise their products as fun and safe for kids, so A.D.'s parents were not overly concerned when they learned of the accounts. But A.D.'s use became problematic as TikTok began flooding her with and encouraging self-harm and

disordered eating. A.D. has received extensive hospitalization for the mental and physical harms caused by her use of these products, and currently weighs under 83 pounds. Her parents are struggling day-by-day to keep their daughter alive and, even though she is only 16, there is no way for them to stop Meta and TikTok from giving her access to their products.

M.L. and N.L. v. TikTok Inc. and ByteDance Inc., Los Angeles County Superior Court, • Case No. 22STCV28204 (filed August 30, 2022) ("M.L. Complaint"). N.L. was 11 when she opened her first TikTok account. TikTok had become popular at her school, and all of the parents understood from TikTok marketing that it was safe for kids and was used primarily for cute, dance videos. Kids were circulating these videos with friends and even parents were taking and posting them with small children. It was advertised as a family app, and its popularity only grew once the pandemic started. Once N.L. was in remote learning, she had access to TikTok for far greater periods of time and TikTok, in turn, began targeting her with extreme, disordered eating subject matters. TikTok's programming of engagement over safety meant that these were the videos from which they believed 11 year old N.L. could not look away - and they were right. It is not at all what N.L. wanted or asked for, but she could not look away and was harmed as a result. N.L. was hospitalized in July of 2021. She weighed 88 pounds and her bloodwork showed that her body was in the process of shutting down. At first, she began to do better - she was attending an all day treatment program that left little time for TikTok. Then another COVID surge happened, N.L. became home bound again, and she turned back to TikTok with the resulting reversal of her recovery. N.L. is now in school full time but has never fully gotten back into recovery and is still struggling and restricting calories. Her mother has taken her to countless health care providers and is spending hundreds in special food every week for her child. It is a day-by-day struggle to keep her daughter alive and even though N.L. recently turned 14, there is no way for M.L. to stop TikTok from giving her access to its product.

3. Suicide, self-harm & content recommender systems

A. Chase Nasca (New York), October 2, 2005-February 18, 2020. 122

Chase was 16 when he died.

Chase had no history of anxiety or depression, a supportive family, involved parents, and close friends, and in late 2021, was accepted to the Olympic Development Program soccer team his third year trying out. He showed no outward signs of depression.

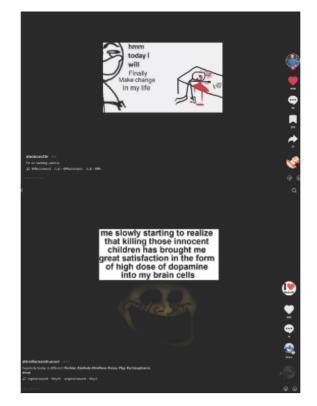
Chase got his first cell phone in 6th grade, after moving to middle school and so his parents could reach him if needed. His parents do not know when Chase opened his first TikTok account, but became generally aware that he had one in 2019 or 2020. TikTok's popularity soared with the onset of the pandemic in March 2020 and, at the time, the only thing they knew about TikTok was that it appeared to be aimed at kids and families and marketed itself as offering silly dance videos that were all the rage. They did not consent to Chase opening a TikTok account, but also had no reason to think that the TikTok product was defective or dangerous in any way.

What Chase's parents know now is that sometime around October 2021, Chase's TikTok took a dark and severe turn. TikTok began sending Chase incredible amounts of suicide, hopelessness, and self-harm themed content. TikTok programmed its algorithm technologies in a manner such that they pushed these videos to Chase despite the fact that Chase was searching TikTok for typical 16-year-old themes like,

Bench Press Tips (December 16, 2021) Kitchen Hacks (December 29, 2021) BoJack Horseman Edits (January 1, 2022) Attack on Titan Opening Song (January 9, 2022) Trae Young Best Moments (January 28, 2022) Motivational Speech (February 5, 2022) Gym Motivation (February 10, 2022) Batman

Instead, TikTok connected Chase to thousands of the most violent and horrific accounts imaginable and exposed him to a never ending stream of suicide promotion. In the three weeks before his death, TikTok was sending these subject matters to chase every single day, and the following are just two examples:

¹²² Dean Nasca et al. v. ByteDance Inc and TikTok Inc., District Court for the Northern District of California, Case No. 5:22-cv-06134 (filed October 18, 2022) ("<u>Nasca Complaint</u>").



Nor was this subject matter Chase wanted or in which he showed interest. For example, on February 5, 2022, Chase searched TikTok for "Motivational Speech." He received and bookmarked one motivational video, but then bookmarked several other suicide promoting videos which were pushed to him by TikTok on his For You Page. The following are just four examples of the text TikTok pushed to Chase the day he sought out "Motivational Speech":

- I can't fucking take it anymore
- Mfs really say "find what makes you happy" i don't want to live
- Might not be able to pull the bitches but i can pull the trigger
- Sleeping is not enough i need to die

TikTok also began sending Chase Nasca videos portraying suicide by standing in front of a moving train, with captions like "Went for a quick lil walk to clear my head." On Friday, February 18, 2022, Chase went to the gym and worked out, stopped at train tracks on his way home, messaged his friend "I can't take it anymore," and stood in front of a moving train.



B. Englyn Roberts (Louisiana), July 26, 2006-September 7, 2020.¹²³

Englyn was 14 when she died.

Englyn was 11 when she got her first cell phone. Her parents were not familiar with social media and did not realize that their daughter would be able to obtain access without their consent. Shortly after she got the phone, however, she began having trouble sleeping and her mom started catching her on the phone at all hours of the night (though she did not realize that Englyn was on social media). Her mom then instituted a rule that the phone had to be turned off by 10:00 p.m., which Englyn agreed to but was then unable to honor due to the level of dependency she already had developed to the Instagram, Snapchat, and TikTok products. Her mom then started taking the phone away at night, but Englyn would sneak into her room after she was sleeping and take it back. Englyn also had strong and uncharacteristic reactions when her mother tried to restrict phone access during the day. She would get anxious and depressed, and would say that could not live without her phone.

Eventually, Englyn's parents learned about her social media use. They were on vacation and Englyn never wanted to go anywhere or do anything without her phone, because she was afraid that she would lose her "streaks." This is when they found out about her Instagram and Snapchat use. However, they had seen these social media products' commercials on TV, and understood that they were relatively safe and harmless for kids. So they allowed her to continue using these products, but did what they could to limit her use at night.

Outwardly, Englyn appeared to be a happy and outgoing child. She had a large family and continued to enjoy spending time with her parents and siblings. She was active and would often sing, dance, and otherwise entertain those around her. She also had a large group of friends and was considered to be very well-liked among her peers. There were no reports or red flags to give her family even a hint of what was coming.

What Englyn's parents learned only after her death was the social media products she was using, Instagram, Snapchat, and TikTok, had targeted her and were exposing her to massive amounts of depression, suicidal ideation, self-harm, and suicide content - horrific, dark, and violent content that was not sent to her because she was interested but, presumably, because as 14-year-old child already addicted to these products she could not look away.

One account to which Instagram connected Englyn Roberts was called **gasstati0nparty**, and featured dark content depicting real people engaged in disturbing and violent acts. In one video, which Englyn and her friend then shared with each other, the user tied an extension cord around her neck and began screaming. These are the types of videos that Meta sends to its young users, and amplifies to garner more likes and comments (a/k/a, engagement from which Meta directly profits).

43

¹²³ Brandy Roberts et al. v. Meta Platforms, Inc. et al., District Court for the Northern District of California, Case No. 4:22-cv-04210 (filed July 20, 2022) ("Roberts Complaint").

On August 29, 2020 (at 3:30 a.m.) Englyn took an extension cord and then took a video of herself crying (no doubt intended for posting on social media). Her parents found their daughter shortly thereafter, after receiving a text from the parent of her friend, and performed CPR until the ambulance arrived. Englyn stayed on life support for nine days, and died on September 7, 2020.

4. Exploitation & user, group and connection recommender systems

A. A.F. (Ohio), born in February of 2011.124

A.F. is an 11 year old child, currently suffering from severe addiction to the Instagram product as well as the harmful effects of severe exploitation and abuse that occurred to her because of Instagram's user recommendation system and other product features.

A.F.'s parents separated in April of 2020, and purchased her a phone so that she could contact each parent while staying with the other. Her parents are not familiar with social media and when she asked if she could open social media accounts they told her no. They believed that this was the end of the issue as she was only 9. They did not consent, and reasonably believed that no one could or would provide a nine-year-old child with a social media account absent parental consent. But Meta did provide her with an account, in fact, it provided her with several. A.F.'s parents believe that she opened, over time, at least six Instagram accounts and possibly more.

A.F. became so locked in to the Meta product that she began staying up at night to use Instagram while her parents slept. She would hide her phone, tell one parent she left it at the other's house, and even break her phone "accidentally" if needed to hide her use. Meta knew that A.F. was using multiple Instagram accounts at all hours of the night, while her parents did not.

Meta has actual knowledge that A.F. opened multiple accounts, and also, that those accounts were opened with different dates of birth. Almost a year ago, A.F.'s father, after discovering and taking possession of three of her Instagram accounts, changed the public profile on one to indicate that A.F. is 11 and that her parents will not allow her to have a social media account. That profile is still public and active.

The A.F. complaint includes detailed examples of how Meta's user recommendation technologies connect and facilitate child sexual abuse and exploitation.¹²⁵ Essentially, Meta's engagement-over-safety programming affirmatively matches children with predators, all but delivering them to their front door. This case also is a rare one in that the parent was able to obtain access to some of the secret accounts; which he was only able to do by physically confiscating the phone after A.F. was caught engaged in sexual acts with adult Instagram users then changing the passwords immediately and before A.F. could access Instagram from a different device. This evidence proves exactly how Meta's product serves up young users to predators for the sake of increasing engagement. On October 16, 2021, Instagram user **Johnny** initiated contact with A.F. and wrote "heyyy." He introduced himself as "houzi from highrise," and asked if this was "another acc you have?" A.F. said yes, she has to "use this one now." He said, "it's fine honey" and told her he only "found [her new account] on accident on my recommended lol." In other words, **Johnny** only found this child on Instagram <u>because</u> of Instagram's user recommendation algorithms and decisions and actions in the programming and

¹²⁴ M.F. et al v. Meta Platforms, Inc., District Court for the Northern District of California, Case No. 4:22-cv-05573 (filed September 29, 2022) ("M.F. Complaint").

¹²⁵ See <u>M.F. Complaint</u>, **¶¶** 187-191.

operating of those algorithms. Johnny and dozens of other adult Instagram users proceeded to exploit and sexually abuse A.F. after Meta directed them to her. Specifically,

- The Instagram account A.F. opened in September 2021 was active for just over one month, during which time A.F. exchanged hundreds if not thousands of messages through Meta's product and interacted with at least <u>twenty-five</u> other Instagram users. Those were people A.F. did not know in real life and most if not all of those users exploited, abused, and/or engaged in commercial sexual acts with A.F.
- The Instagram account A.F. opened in October 2021 was active for less than two weeks, during which time A.F. exchanged hundreds if not thousands of messages through Meta's product and interacted with at least <u>forty-four</u> other Instagram users. Those users were people A.F. did not know in real life and most if not all of those users exploited, abused, and/or engaged in commercial sexual acts with A.F.

Most if not all of these adult, male users would not have found A.F. but for Meta's product features and programming of those product features.

B. Selena Rodriguez (Connecticut), 2009-2021126

Selena Rodriguez was given an iPad at age 9 to play games on the internet. She opened Instagram, TikTok, and Snapchat accounts without her mother's knowledge or consent, and her social media use became obsessive and harmful in a short period of time. She used social media for several hours every day, including most nights and into the morning, and became violent when her mother tried to take her devices away from her. She developed body issues, depression, and suicidal ideation, as well as severe sleep deprivation and related harms. Her mother knew about one Instagram account and Meta has recently disclosed in litigation that there were at least seven others. Predators found her on Instagram and Snapchat because of Meta's user recommendation algorithms, and exploited and abused her. She was subjected to online bullying, and harassment after exchanging explicit photos on Snapchat - which she only agreed to because she believed Snap's representation that photos disappeared. She was exposed to depressive and self-harm subject matters on Instagram and TikTok, sent to her as a direct result of the companies' engagement over safety programming decisions.

On July 21, 2021, Selena filmed and posted to Snapchat a video of herself taking two pills, and made the peace sign. Shortly thereafter, she died of acute bupropion intoxication. She was only 11 at the time.

¹²⁶ Tammy Rodriguez v. Meta Platforms, Inc. et al, United States District Court for the Northern District of California, Case No. 3:22-cv-0401-JD (original Complaint filed January 20, 2022) ("<u>Second</u> <u>Amended Rodriguez Complaint</u>").

5. Snapchat's misrepresentations about disappearing images

A. Sarah Flatt (Tennessee) October 24, 2004 - September 4th 2019

Sarah Flatt¹²⁷ was 14 years-old when she died by suicide (on September 4, 2019). Sarah believed that photos she sent via Snapchat would disappear and was proven wrong, resulting in explicit photos being sent to her school and community. Sarah's father confiscated her phone and, almost immediately thereafter, Sarah took her own life.

B. A.C. and his son, John Doe

A.C. is a web developer. As his son got older, A.C. believed that he had the technical knowledge and experience to ensure a safe social media experience for his son. However, even the most technically savvy parent cannot stop social media companies as currently operated from providing children access to social media accounts. When A.C.'s son was younger, he was able to open accounts by sneaking access to devices and, on one occasion, using a gift card to buy a phone online without his father's knowledge. A.C. (being familiar with these technologies and the known dangers of the internet) spoke to his son often about responsible use of any sort of internet communication tool.

When A.C.'s son was 14, a predator found him on Instagram via the public profile settings Instagram allows for minor accounts. The predator posed as a beautiful young woman and convinced A.C.'s son to exchange explicit photos via Snapchat, which he eventually agreed to based on his belief that his Snaps would disappear (which is how Snapchat markets its product). The predator, however, was able to save his photos and videos and immediately demanded money, under the threat of circulating those to the minor's classmates and family on social media. A.C.'s son tried everything possible to shut out the predator, including blocking the user on Snapchat and Instagram and changing his profile name and information, but the predator was always able to find and contact him. The predator then started a group chat within Instagram and began adding several of the minor's classmates and family members, telling these other users that they were about to expose the minor.

The minor told his father, a web developer experienced in all things technology. A.C. was confident based on his understanding of how these products worked that he would be able to reach out to Meta and promptly put a stop to the incredible harms that were occuring and were about to occur to his son, and also ensure that the Instagram predator was banned from utilizing Meta's products to harm other young children. A.C. utilized his son's Instagram account and his own Instagram account to begin reporting these harms, again, confident that Meta would act (as consistent with Meta's own terms of service) to prevent any further harm from occurring. What A.C. soon learned, however, is that Meta does not provide a 1-800 number or any form of staffed reporting mechanisms for users or their parents to report harm directly. A.C. scoured the internet for information on Meta's product and reporting mechanisms, and learned that Meta does not

47

¹²⁷ Gail Flatt v. Meta Platforms Inc. et al., District Court for the Northern District of California, Case No. 3:22-cv-04535 (filed August 5, 2022) ("Flatt Complaint").

provide that information to consumers - making it incredibly difficult for someone even as savvy as A.C. to submit reports and ensure that those reports are getting where they need to go.

353

On May 14, 2022, A.C. made his first series of reports to Meta about the predatory user, as well as the group chat and the fact that Meta needed to intercede to stop the predatory user from circulating explicit photos of his minor child to classmates and family. A.C. checked Instagram nonstop for updates, only to find that the offending account was still active and only to learn that Meta had done nothing to stop that user from adding more of his son's contacts to the group chat on Instagram to circulate explicit photos of his child. It took Meta four days before the predatory user's account no longer appeared on Instagram, but even then, A.C. could not obtain assurances from Meta that the account and group chat page had been taken down. In fact, the messages Meta was sending to his account reported that his report was still being reviewed and that it could not be reviewed due to "a technical issue" - depending on whether A.C. checked Instagram via the app or a web browser.

In the meantime, A.C. discovered that this predatory user was opening new accounts and/or had multiple Instagram accounts, all with the appearance of credibility as the predator had been able to amass hundreds (in some cases more than a thousand) followers. These accounts utilized some combination of the same photographs and usernames, and were identifiable to A.C. in a matter of minutes. Yet Meta was allowing these secondary accounts, despite having taken down at least one account for severe violations of Meta's terms and distribution of CSAM. Knowing that this predatory user was likely harming other children in the same manner, A.C. began reporting the secondary accounts. In some instances, he had to make several reports before he could get through and often Meta's links as provided at its Help Center and similar locations simply did not function. In some instances (usually after several reports and pleas), Meta would send an automated message saving that it had taken down the account. In other instances (after the same reports and pleas), Meta would send an automated message saying that it was not taking action because the account did not violate its community standards. Never once was A.C. able to get Meta to provide him with a phone number or human being with whom he could discuss what was happening. A.C. sent Meta a news article detailing a young man who had recently died by suicide after being exploited in virtually the same manner as his son was exploited. Yet still, there was no way for him to speak to a human being at Meta.

To this day, the predator user has live accounts on Instagram which are likely being used to exploit and harm children. A.C. has sent information to Meta through every available and presumably working reporting mechanism Meta provides - which mechanisms are confusing, complicated, and time consuming on a good day, and outright broken at other times (resulting in error and technical difficulty automated responses). Even when A.C. does get a report to process, Meta's responses are inconsistent and in at least some cases Meta has opted to allow the known predator to continue using its product.

A.C. is a web developer, with years of experience in the field of technology. Meta has implemented a system that even he cannot successfully and reasonably navigate, despite having spent dozens of hours trying. A.C. has documented every step he took and harms Meta caused in connection with these events. A.C. would never have let his son use Instagram had Meta disclosed the defects in its product and reporting mechanisms, including but not limited to its

orts ai

failure to provide for reasonable reporting mechanisms and the fact that Meta will not enforce its own safety-related community guidelines and terms when it comes to prohibiting illegal activity on its platform and blocking known predators.

6. The extremities young people are going to to get a break from social media

A number of SMVLC clients have gone to extreme lengths to take a break from social media and to make it stop even for a short while. This includes having themselves committed.

For example, N went to the extreme length of getting herself admitted to hospital in order to take a break from the addictive nature of social media. Equally disturbing is the nature of the harm N was trying to "take a break" from.

N began using social media when she was around 10 or 11. She quickly became addicted to Instagram, Snapchat, and TikTok, followed by sleep deprivation, anxiety, depression, academic struggles, and other related harms. She was using Snapchat's My Eyes Only product which hid and deleted evidence of grooming, including from her parents. Multiple men had found N via user recommendation features and to engage with her in ways that no-one could see because of the My Eye's Only feature. On one occasion, she told her mother that she wanted to hurt herself and needed to be taken to the hospital because she did not trust herself to not follow through. The hospital admitted her for treatment but did not allow her to take her phone. This enabled N's mom to see her social media feed, including My Eyes Only, where she could see that several adult males were actively grooming N. She also found a conversation in which her daughter said that she *needed a break from one of the adult males constantly messaging her through these apps, and that she planned to get herself checked into a mental hospital to get that break.*

Tragically, many SMVLC clients who have taken their own life left suicide notes that echo this theme. Given the dominant and problematic relationship all had with social media, it's difficult not to read these as desperate statements about their inability to cope with social media or to take it any longer.

 \bigcirc