S. HRG. 117–707

PROTECTING KIDS ONLINE: INTERNET PRIVACY AND MANIPULATIVE MARKETING

HEARING

BEFORE THE

SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, AND DATA SECURITY

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

MAY 18, 2021

Printed for the use of the Committee on Commerce, Science, and Transportation

Available online: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
53–091 PDF WASHINGTON : 2023

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

MARIA CANTWELL, Washington, *Chair*

AMY KLOBUCHAR, Minnesota
RICHARD BLUMENTHAL, Connecticut
BRIAN SCHATZ, Hawaii
EDWARD MARKEY, Massachusetts
GARY PETERS, Michigan
TAMMY BALDWIN, Wisconsin
TAMMY DUCKWORTH, Illinois
JON TESTER, Montana
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
BEN RAY LUJÁN, New Mexico
JOHN HICKENLOOPER, Colorado
RAPHAEL WARNOCK, Georgia

ROGER WICKER, Mississippi, *Ranking*
JOHN THUNE, South Dakota
ROY BLUNT, Missouri
TED CRUZ, Texas
DEB FISCHER, Nebraska
JERRY MORAN, Kansas
DAN SULLIVAN, Alaska
MARSHA BLACKBURN, Tennessee
TODD YOUNG, Indiana
MIKE LEE, Utah
RON JOHNSON, Wisconsin
SHELLEY MOORE CAPITO, West Virginia
RICK SCOTT, Florida
CYNTHIA LUMMIS, Wyoming

DAVID STRICKLAND, *Staff Director*
MELISSA PORTER, *Deputy Staff Director*
GEORGE GREENWELL, *Policy Coordinator and Security Manager*
JOHN KEAST, *Republican Staff Director*
CRYSTAL TULLY, *Republican Deputy Staff Director*
STEVEN WALL, *General Counsel*

SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, AND DATA SECURITY

RICHARD BLUMENTHAL, Connecticut, *Chair*
AMY KLOBUCHAR, Minnesota
BRIAN SCHATZ, Hawaii
EDWARD MARKEY, Massachusetts
TAMMY BALDWIN, Wisconsin
BEN RAY LUJÁN, New Mexico

MARSHA BLACKBURN, Tennessee, *Ranking*
JOHN THUNE, South Dakota
ROY BLUNT, Missouri
JERRY MORAN, Kansas
MIKE LEE, Utah
TODD YOUNG, Indiana

CONTENTS

PROTECTING KIDS ONLINE: INTERNET PRIVACY AND MANIPULATIVE MARKETING

TUESDAY, MAY 18, 2020

U.S. SENATE,
SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, AND DATA SECURITY,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10:01 a.m., in room SR–253, Russell Senate Office Building, Hon. Richard Blumenthal, Chairman of the Subcommittee, presiding.

Present: Senators Blumenthal [presiding], Klobuchar, Markey, Luján, Blackburn, Thune, Lee, and Young.

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

Senator BLUMENTHAL. Welcome to this hearing, Protecting Kids Online. I want to thank Ranking Member Blackburn and our witnesses for being here today. Her collaboration has been invaluable, and I am looking forward to the excellent observations that we will hear from you and from the United Kingdom.

As children spend drastically more time online, the tech platforms really have become a perilous mine field for many of them. They are deeply addictive and potentially destructive without sufficient parental supervision or safeguards. I fought for data privacy rules for consumers and accountability for tech companies, focusing on the harms that they cause. Nowhere is that more profound and urgent than for children.

Big Tech and data brokers are spying on children, watching them play, monitoring their lives. No company should be allowed to collect permanent, invasive dossiers on our children. Even more concerning are the cesspool of illicit pitches to kids. In a survey last week, by the antihuman trafficking organization, THORN, the finding was that more than a quarter of children nine to 11 years old receive sexual solicitations on social media, often by adults. A quarter of those children receive sexual solicitation.

These children are also assailed by aggressive, sophisticated, and undisclosed marketing that prey on their impressionable minds, and exploit those dossiers of private information for commercial gain. Two examples, one TikTok, the other Instagram. According to THORN, 66 percent of young children, nine to 12 years old, use the video sharing app, TikTok. It can often be informative and entertaining. It has held itself out to parents to be safe. But it has aggressively recruited young users.

Regrettably, TikTok has a troubling track record on children's privacy. Only 2 years ago, TikTok paid a then record $5.7 million fine for disregarding our children's privacy rules and illegally collecting data about kids. It then shared this sensitive information with third parties and advertisers. This practice still continues. In March 2020, children's advocates, led by Professor Campbell, filed a complaint with the Federal Trade Commission, alleging TikTok continues to violate the law. TikTok is also facing investigations in Europe, for failing to protect children.

Privacy is not the only issue. Organizations like the National Center on Sexual Exploitation and the Center for Digital Democracy have all raised concerns about predatory sexual content and manipulative advertising on TikTok. The FTC even called attention to TikTok being used by predators to groom nearby children, in its case against the company.

Because TikTok is so popular with young audiences, Ranking Member Blackburn and I invited the company to this hearing. We asked them to come in and explain how they are safeguarding children. Parents deserve to hear from TikTok, and I am disappointed that TikTok rejected our invitation and refused to discuss these issues with Congress. We are going to continue to invite them to come. I hope that they will give parents and Congress the explanations we deserve. They have been failing to do it.

I am also alarmed by Facebook's recent announcement that it will launch a version of Instagram marketed to children. Instagram has a notorious record of disinformation, bullying, and deception. Prominent Instagram influencers often push alcohol, tobacco, and other dangerous products on young fans, despite warnings from the FTC.

Sexual exploitation is also a problem. According to THORN, 16 percent of children and teens that have been sexually harassed on Instagram, tied with Snapchat for the most reports of harm. I have no trust, none, that Facebook will keep these young users safe. It has failed far too often. For example, one design flaw in its Messenger Kids app allowed strangers to chat with children. Given that record, I cannot imagine why Facebook would bulldoze ahead into kids' lives.

Senator Markey and I wrote to Facebook, asking questions about its plans and we have received woefully inadequate answers. I agree that—I agree with the 44 State Attorneys General, and dozens of child welfare specialists saying, no. Facebook should abandon its plans for Instagram Kids. Facebook should stop this additional intrusive, and potentially dangerous, interference in kids' lives and abandon plans for Instagram Kids.

As for the way forward, we must stop these business practices, corporate negligence, and commercial exploitation of children that now exists online. Spying and preying on children is never OK. Parents are powerless to prevent it now. They need the tools to stop it themselves, or Congress must intervene to end it.

I commend my colleagues, Senators Markey and Cassidy, for introducing the bipartisan Children and Teens Online Privacy Protection Act. I worked on this issue with them, and I will be strongly supporting and advocating such measures.

But we need to do more. The EARN IT Act, that Senator Graham and I introduced last session, approved unanimously by the Senate Judiciary Committee, offers a template for even broader action on Section 230. Eventually, the tech platforms must be held accountable. They must bear liability for obvious violations of criminal and perhaps civil law. And the cutbacks in Section 230 immunity, carefully tailored to meet the needs of harm to children, offer a very important path forward.

And I also commend the trailblazing work of Baroness Kidron to draft an age-appropriate design code and an online safety bill in the United Kingdom. It, too, offers a potential model for us.

I now turn to Ranking Member Blackburn.

STATEMENT OF HON. MARSHA BLACKBURN,
U.S. SENATOR FROM TENNESSEE

Senator BLACKBURN. Thank you, Mr. Chairman. And I want to welcome our witnesses, Mr. Egelman, Ms. Campbell, who are with us in person, and Baroness Kidron, who is joining us remotely today. And to our staffs who have worked on this issue, I thank you for doing the work to put this hearing together.

Mr. Chairman, I join you in being disappointed with how TikTok has refused to appear before us and remain disappointed and really frustrated with them and their lack of attention to data security, to children's privacy. And it seems that TikTok is proving to be incapable of doing the right thing, to protect our children.

The Internet has completely revolutionized how our society functions. Anything you could ever want, or need can be found online. This has made the Internet a logical tool for parents and teachers to help educate and entertain their children through online services and streaming platforms. Children born today will spend more time connected online than any other past generation.

Companies use advanced data collecting techniques to gather and analyze the habits, movements, and interests to build at a virtual view that only exists to cater to advertisers.

While I have spoken on this before, the impact this has on children can be even more detrimental. By taking advantage of the "always on" mentality, children are constantly being tracked and analyzed. Take TikTok, for example. They have been accused of using algorithms to keep kids scrolling indefinitely. Alphabet, Google and YouTube's parent company, has been accused of tracking children when they are not using their school devices and using features, such as auto play, to keep kids glued to their devices.

But this does not end with tracking and scrolling. Companies like Snapchat have exposed children to predators and explicit adult content, while using their products. With millions of teen users, disappearing messages, and a map of all of your contacts, this has become a child predator's dream.

Instagram, which Facebook owns, announced that they were going to create an Instagram for kids, but was immediately met with backlash from over 40 states, including Tennessee.

As time moves forward, children will be at the forefront of technology, with each generation being more connected than the last. That is why it is so important that we get this right. We must ensure that children are not being taken advantage of and molded

into something that they are not. Social media is causing our children to become more distressed than ever before. Do not take my word for it. Go talk to any pediatrician.

Companies exploit children's desire to connect with their peers, utilizing behavioral design tools that are highly addictive. Young girls, in particular, are susceptible to body image issues and decreased self-esteem, from the distortions of reality present on many of these platforms.

With so many children engaging in remote learning during this pandemic, it is more important that we remain vigilant, as parents and grandparents. We must not forget to focus on protecting their virtual you, as we work to craft comprehensive privacy legislation. Last Congress, Senators Wicker, Thune, Fischer, and I introduced the SAFE DATA Act, which contained a requirement that companies not transfer the data of individuals between the ages of 13 and 16, without the expressed consent of that individual, or of their parent or guardian.

I am pleased to see continued engagement on this important topic, and I look forward to working with the members of this committee to craft legislation to help protect our precious children from Big Tech.

Thank you, Mr. Chairman.

Senator BLUMENTHAL. Thanks, Senator Blackburn. I do not know whether Senators Cantwell or Wicker have any comments remotely. I guess not. I would like to now introduce the witnesses and we are very pleased to have you here today.

Professor Angela Campbell, Professor Emeritus at Georgetown Law School. Professor Campbell is the Chair of the Board of the Campaign for Commercial-Free Childhood. She is also Professor Emeritus at Georgetown Law's Institute for Public Representation. She received her JD from the University of California, Los Angeles, and her BA from Hampshire College.

Dr. Serge Egelman, Research Director of Usable Security and Privacy Group, International Computer Science Institute, University of California, Berkeley. Dr. Egelman leads the University of California's Berkeley Lab for Usable and Experimental Security, known as BLUES. He—his research focuses on the intersection of privacy, computer security, and human-computer interaction, with the aim of better understanding how people make decisions surrounding their privacy and security, and then, creating data-driven improvements to systems and interfaces.

He received his PhD from Carnegie-Mellon University and his BS from the University of Virginia.

We are also joined, remotely, by Baroness Beeban Kidron, Founder and Chair, 5Rights Foundation. Baroness Kidron is the Founder and Chair of that organization, a foundation dedicated to making systematic changes to the digital world, to ensure it caters for children and young people, by design and default. She is a crossbench member of the House of Lords, and sits on the Democracy and Digital Technologies Committee.

She introduced the age-appropriate design code, the first standalone data protection regime for 18 into UK law. She is also a commissioner for UNESCO's Broadband Commission for Sustainable

Development, where she is a member of the working group on child online safety.

Thank you all for being here today. We will begin with testimony from Dr.—Professor Campbell.

STATEMENT OF ANGELA J. CAMPBELL, CHAIR, BOARD OF THE CAMPAIGN FOR A COMMERCIAL-FREE CHILDHOOD; PROFESSOR EMERITUS, GEORGETOWN LAW

Ms. CAMPBELL. Thank you. I want to thank Chairman Blumenthal, Ranking Member Blackburn, and the distinguished members of the Subcommittee, for inviting me here to testify about protecting children online. I am, as Senator Blumenthal said, Chairman of the Board for the Campaign for a Commercial-Free Childhood, a leading watchdog of the children's media and marketing industries. Its advocacy is based on overwhelming evidence that child-targeted marketing and the excessive screen time it encourages, undermines kids? healthy development.

CCFC led the charge in filing a complaint against YouTube for violating COPPA, that eventually led to the FTC's 2019 settlement, which included a record fine of $170 million and it limited the collection and targeted advertising on child-directed content on YouTube. Most recently, CCFC worked with a coalition of advocates and sent a letter to Facebook, urging them to drop their plans to offer Instagram for kids.

My testimony also draws on my over 30 years' experience as the directing clinic at Georgetown, where we actually filed the very first complaint with the FTC ever, about a website that was targeting children, alleging that they were engaging in unfair and deceptive practices. And after a lot of hard work by many people, including then-Representative Ed Markey, Congress passed the Children's Online Privacy Protection Act, or COPPA. I am extremely proud of this accomplishment and I think it has provided significant protections for children, but it is badly in need of updating.

In my written testimony, I address three issues, two of them I will leave for the questions. That is why children and teens need more protection against unfair and deceptive advertising practices online. And also, my suggestions about what the FTC could do to better protect children.

So now, I will focus on why COPPA needs updating and how it should be updated. When COPPA was adopted in 1998, there was no YouTube, there was no social media, there were no smartphones, no smart speakers, and no Internet of things, including toys, connected to the internet. At that time, children's use of screens primarily consisted of watching broadcast or cable television. But today, as you have noted, they use digital media for education, entertainment, and socializing, and they spend many hours a day using these devices. And this time, of course, has only increased with the pandemic.

As children and teens viewed—shifted their viewing from television to digital devices, marketing also became digital, and much more powerful. It uses incredibly sophisticated and elaborate systems to deliver targeted advertisements. The advertisers are able to track the users online, across multiple devices, combine that data with other data from other sources, and use very powerful al-

gorithms and machine learning, to decide what—in real time, what ads an individual will see. This system allows kids to be profiled, for example, as gamers or impulsive purchasers or anxious over sharers, and then, targeted with ads designed to manipulate them to do more of those things.

The dominant business model is for the platforms to keep the children engaged as long as possible, because then, that way, they will see more ads and the platforms can collect even more data about them. This unregulated business model harms young people, whose developing cognitive capabilities are no match for today's highly sophisticated digital marketing tactics.

While it is profitable for the platforms, it means that young people are spending a lot of time online and they are often viewing things that may not be appropriate for them or, as you mentioned, getting—being solicited for inappropriate purposes. Time online has also been associated with a number of different problems, including depression and mental health, poor nutrition, insufficient sleep, problems in school, cyberbullying, online sexual abuse, risky behavior, and in some cases, even suicide.

The COPPA rule that the FTC adopted and amended in 2013, generally prohibits targeting the profile of children under age 13, unless parents having given notice about what data is collected, how it will be used, and with whom it will be shared, and have given advanced verifiable consent. However, the rules—these protections only apply in two situations. First, where a website or online services is directed at children. And second, where the operator has actual knowledge that it is collecting data from a child.

Now, it is difficult to know whether or not a service is directed to children. And of course, children do not limit themselves to using only services directed at children. They use sites that are directed to mixed audiences or general audiences, as well. And so, when they are doing that, they are not covered by the protections, unless the company has actual knowledge. This actual knowledge standard is very problematic because it incentivizes operators to avoid complying with COPPA by saying—by not knowing, or pretending not to know, that children are using their platform.

This is exactly what YouTube did until the FTC finally brought some enforcement action. Even though YouTube was, and is, the most popular online destination for children, Google insisted, for years, that YouTube had no COPPA obligations because its terms of service said the service was for 13 and above.

Similarly, today, TikTok's terms of service says it is for only 13 and above and yet, it has internally classified one-third of its users as younger than 14. And this is true even though they are already subject to this consent decree with the Federal Trade Commission, to make sure that they comply with COPPA.

So, I think part of the problem with actual knowledge is, that it is really hard to prove. While in these two big cases, the FTC did conduct investigations and it did find actual knowledge, companies know that the FTC rarely initiates investigations. In fact, in 21 years, there have been 34 enforcement actions brought by the FTC. And it is very difficult to prove actual knowledge. It is a subjective standard which has to examine what the relevant people knew when. It is information that is not public and there are many dif-

ferent parties involved in serving ads to kids. And many of these decisions are made by machines, by computers.

So, it is important to replace the objective standard with constructive knowledge, which essentially means that the operator knew or should have known. It imposes a duty of reasonable care on the operators to determine whether they are collecting data from children. And I am very pleased that the Children and Teens Online Privacy Protection Act, which was introduced by Senators Markey and Cassidy, would replace actual knowledge with constructive knowledge. And it also makes clear what that means in the context of the digital ecosystem.

Now, the other big problem with COPPA is that it only applies protections to children under age 13. Once a child turns 13, he or she is treated just like they were an adult. The teens are not developmentally the same as adults. They are still developing their capacities for self-regulation. They are wired to seek approval from their peers, and they lack the experience and judgment to assess risks and understand long-term consequences.

With teens spending, on average, seven and a half hours per day on social media, playing video games, and watching videos, this means they are developing their social and personal identities online. And apart from the harms that I have already mentioned, this data can be used—the data collected from all of these activities can be used to effect their future opportunities, such as, whether and where they go to college.

The Children and Teens Online Privacy Protection Act, as well as the KIDS Act, which was introduced last session by Senators Markey and Blumenthal, would extend developmentally appropriate protections to minors, defined as ages 13 to 15. It would allow operators to collect personal data from minors, only if they adopt and follow a digital marketing bill of rights for minors, that is consistent with the fair information practices set forth in the legislation. It would also prohibit targeted marketing to minors, unless the minors were given sufficient notice and gave affirmative consent.

So, I see that my time is about out and so, I will leave the other areas that I wanted to talk about, which is the need to apply protections against unfair and deceptive advertising, and other things that the FTC could do, to the questions. Thank you and I am happy—look forward to answering your questions.

[The prepared statement of Ms. Campbell follows:]

PREPARED STATEMENT OF ANGELA J. CAMPBELL, CHAIR, BOARD OF THE CAMPAIGN FOR A COMMERCIAL-FREE CHILDHOOD; PROFESSOR EMERITUS, GEORGETOWN LAW

Chairman Blumenthal, Ranking Member Blackburn, and Distinguished Members of the Subcommittee: Thank you for inviting me to testify about protecting children online. I am pleased that the Subcommittee is focusing on the important issues of children's online privacy and manipulative marketing to children.

I am here in my role as the Chair of the Board of the Campaign for a Commercial-Free Childhood. CCFC is the leading watchdog of the children's media and marketing industries. CCFC's 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 legal filings, CCFC has changed the child-targeted marketing and data collection practices of some of the world's biggest companies. Most notably, CCFC's 2018 complaint filed with the FTC against YouTube ultimately led to the 2019 FTC settlement that re-

quired YouTube to pay a record fine and to limit data collection and targeted advertising on child-directed content. CCFC is currently leading a large coalition of parents, advocates and child development experts urging Facebook to abandon its plans for a kids' version of Instagram.[1]

My testimony also draws on my over 30 years as the director of a clinical program at Georgetown Law that represents nonprofit organizations, including CCFC and the Center for Digital Democracy, advocating for media policies in the public interest. In this capacity, I supervised the drafting of numerous comments and requests for investigation filed with the FTC concerning children's advertising and privacy.[2] In 1996, the clinic filed the first complaint alleging that a website directed to children was engaging in unfair and deceptive practices. This complaint that focused attention on the need to protect children's online privacy, and with much hard work by many people including then-Representative Markey, Congress passed the Children's Online Privacy Protection Act (COPPA) in 1998. I am extremely proud of this accomplishment and the important safeguards COPPA has provided for children. Today, however, COPPA badly needs updating.

In this testimony I addresses three issues. First, I will discuss why it is urgent to update COPPA and the key areas where the current protections have fallen short. Next, I will explain why we need greater protections for children and teens against unfair and deceptive advertising practices online. Finally, I offer suggestions about how the FTC could better protect children.

I. New privacy legislation is needed to protect children and teens

When COPPA was adopted in 1998, there was no YouTube, no social media, no smartphones, no smart speakers in children's bedrooms, and no toys connected to the internet. Today, children and adolescents increasingly use digital media for education, entertainment, and socializing. Prior to the pandemic, research by Common Sense found children in the U.S. from birth to age 8 consumed an average of two and a half hours of screen media a day, while 8- to 12-year-olds averaged just under five day, and teens averaged about seven and a half hours—and these figures do not include use for school or homework.[3] The pandemic has accelerated these trends, with studies reporting screen time up as much as 50 percent.[4]

Moreover, over the last twenty years, an incredibly sophisticated and elaborate digital marketing ecosystem has developed. The boundaries between programming and marketing have completely eroded so that even discerning adults have difficulty identifying what is sponsored content. In addition, no longer do viewers of the same content see the same ads, as they did with traditional television and print advertising. Marketing has become personalized to appeal to the particular interests of individuals. This type of marketing, often called targeted or behavioral advertising, is made possible by tracking users' online activity across multiple devices, combining data from multiple sources, and using algorithms and machine learning to make inferences about what users want or are likely to respond to.

Targeted marketing makes it harder for parents to monitor what their children are seeing. Moreover, most Americans are not aware of the extent of data collected online and how it can be used to manipulate them. Because the problems are system-wide, there is little parents can do on their own to protect their children. Thus, regulatory intervention is urgently needed. I am pleased that the subcommittee is considering legislation to better protect children.

A. The unregulated system of digital media is harmful to children

The largely unregulated business model for digital media subjects young people to three types of interrelated harms.

First, a large body of research demonstrates that children's and adolescent's developing cognitive capacities are no match for today's highly sophisticated digital marketing tactics, which leverage enormous data sets, machine learning, and the most powerful persuasive technologies ever created, to deliver in real time an advertisement that a young person is most vulnerable to at a given moment. 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."[5]

These concerns are not theoretical. In 2017, leaked documents revealed that Facebook boasted to advertisers that it could target teens at the exact moment they were feeling bad about themselves, including when they have negative thoughts about their bodies.[6] This year, advocates were able buy Facebook ads targeted to teens who are interested in alcohol, gambling and extreme weight loss.[7] Not surprisingly, given both the inherent unfairness of personalized marketing to children and the fact that kids and teens are often targeted with ads for harmful products, marketing is a factor in many of the most pressing problems facing children today, in-

cluding childhood obesity, body image issues, a rise in materialistic values and family conflict.

A second harm is that the vast amount of data collected from young people is used to deliver the personalized content that is most likely to keep them on a platform. While maximizing engagement generates profits for platforms, the overuse of digital media it encourages is particularly harmful to young people. It has been associated with, among other things, depression and mental health problems, poor nutrition, problems in school, cyberbullying, insufficient sleep, and online sexual abuse.

Finally, spending so much time using digital devices exposes young people to harmful and inappropriate content. The platforms want young people to stay online as long as possible because it increases their profits. They use algorithms to recommend the content that is most likely to keep kids engaged, regardless of whether that content is educational, age-appropriate or promotes prosocial behavior. As a former YouTube engineer explains, "Recommendations are designed to optimize watch time, there is no reason that it shows content that is actually good for kids." [8]

B. In practice, COPPA's actual knowledge standard permits the collection of personal information from children and is difficult to apply

COPPA needs to be amended to address these harms. Experience over the last twenty years has shown that a significant weakness of COPPA is that its protections apply only to websites and online services that are considered *directed to children,* or where the operator has *actual knowledge* that a child or children under thirteen is using their site or service. Yet many sites and services directed to mixed and general audiences are nonetheless used by many children.

COPPA's actual knowledge standard creates a giant loophole that undermines children's safety. It incentivizes platforms to avoid COPPA compliance by not knowing—or pretending not to know—that children under thirteen are using their platforms. For example, even though YouTube is the most popular online destination for children, Google insisted for years that YouTube had no COPPA obligations because the platform's Terms of Service said it was for ages thirteen and up. Similarly, TikTok continues to claim it lacks actual knowledge of accounts belonging to children under thirteen—despite that fact that TikTok has used machine learning to classify one-third of its users as younger than fourteen.[9]

While YouTube and TikTok clearly had actual knowledge of children using their platforms, the FTC had to conduct investigations to prove it. Companies know that the FTC rarely initiates investigations. Moreover, even when the FTC investigates, it can be difficult to prove "actual knowledge." A single child-directed app, for example, may be sending a child's personal information to dozens of firms that engage in targeted advertising, monetization and analysis.[10] Because of the many parties involved in online data collection and marketing and because many decisions are made by algorithms rather than humans, the actual knowledge standard, which requires the FTC to show what operators actually know, is unworkable.

The Children and Teens' Online Privacy Protection Act, introduced by Senators Markey and Cassidy, would close this loophole in COPPA by making an operator liable if it has "constructive knowledge that personal information is being collected from a child or minor." "Constructive knowledge" is an often-used legal concept that generally means that one "knew or should have known." Constructive knowledge is an objective standard, and it relies on facts ascertainable by the FTC and the public and can be determined without needing to know what the party in question was actually aware of or intending to do. A constructive knowledge standard would impose a reasonable duty of care on operators to determine whether they are collecting data from children, and if so, provide appropriate safeguards.

C. COPPA lacks any protections for adolescents

Another huge loophole in COPPA is that it only applies for children under age 13. Once a child turns 13, he or she is treated the same as an adult. I am not aware of any other legal context in which thirteen-year-olds are treated as adults. Increasingly, the US' lack of protections for teens puts it at odds with the trend in Europe and elsewhere to offer special data protections for young people until they turn at least 16, and in some cases, up to 18. More than 90 percent of U.S. parents believe COPPA's protections for children should be expanded to teens.

Teens are vulnerable online for different reasons than younger children. Not only do they spend more time online, but adolescence is the period of personal and social identity formation. Much of this development is now reliant on social media. Because teens have a limited capacity for self-regulation compared to adults and are vulnerable to peer pressure, they often find it difficult to identify and respond appropriately to online risks. Excessive social media use by teens has been associated with a wide variety of public health issues including depression and mental dis-

orders, exposure to unwanted to explicit content, harassment, sexual solicitation, bullying, self-harm, and even suicide.

The Children and Teens' Online Privacy Protection Act, as well as the KIDS Act, which I discuss below, would extend developmentally-appropriate protections to minors, defined as ages 13 to 15. Specifically, it would prohibit operators from collecting personal data from minors unless the operator adopts and follows a Digital Marketing Bill of Rights for Minors that is consistent with the Fair Information Practices Principles set forth in Section 4 of the bill. It would prohibit targeted advertising to minors unless the minor is given notice and gives affirmative consent. Minors would also have the right to delete personal information displayed on a website, online service, and online or mobile apps, which they had submitted.

D. Targeted advertising to children should not be permitted

COPPA currently allows parents, after receiving appropriate notice and granting affirmative verifiable consent, to permit the collection of a child's data for the purposes identified in the notice. The FTC's COPPA Rule as amended in 2013 prohibits targeted advertising to and profiling of children absent parental notice and consent. However, in practice, targeted advertising to children remains widespread.

As described above, the harms from targeted advertising—both from the ads themselves and the ways behavioral advertising shape children's online experiences—are serious enough that Congress should explicitly prohibit the practice when aimed at children. The Children and Teens' Online Privacy Protection Act would do just that by making it unlawful for operators to use, disclose, or compile children's personal information for the purposes of targeted marketing.

I hope that the subcommittee will quickly adopt these important revisions to COPPA as set forth in the in Children and Teens' Online Privacy Protection Act.

II. Legislation is needed to prevent unfair and deceptive marketing to children and teens

I hope that the subcommittee will also consider legislation similar to the KIDS Act (S. 3411) introduced by Senators Markey and Blumenthal in the last session. The KIDS Act would offer children protections from unfair and deceptive marketing on online platforms, similar to those that currently exist for television and discourage certain other practices harmful for children.

It has been understood since the mid-1970s that children are more vulnerable to advertising than adults. Research on television advertising has consistently found that children under the age of 8 have difficulty understanding advertising's persuasive intent and it is not until around age 12 that children begin to understand that advertising is designed to change their behavior. When advertising is embedded in programming—which is often the case on the Internet—children's and teens ability to even identify advertising, let alone think critically about it, is likely to emerge even later.[11] More than 90 percent of U.S. parents believe COPPA's protections for children should be expanded to teens.[12]

For this reason, the Federal Communications Commission has long required restrictions on advertising on children's television programming to help mitigate young people's vulnerabilities to marketing. These include a clear separation between program content and advertising, a prohibition of the use of certain unfair and deceptive advertising methods such as host selling and embedded advertising, and limits on the total amount of advertising that can be shown.

Over the years, however, children's viewing behavior has changed. They are watching less traditional broadcast and cable television and spending more time online watching online videos, playing Internet and mobile games, and interacting on social media. Unfortunately, there is no equivalent to the FCC policies for children's television on the internet.

As a result, much of the content that children and teens view online today is marketing. In addition to pop-up and banner ads, marketing is embedded into content in such a way that children don't recognize that they are being marketed to. And that is the point. Children and teens say they don't like advertising, and embedded content can't be blocked by ad blockers. Thus, covert advertising is more effective than traditional forms of advertising.

Covert advertising occurs in many forms and is known by different names such as influencer marketing, native advertising, product placements, and unboxing videos. Influencer marketing, for example, takes place when brands pay or reward social media influencers for promoting their products online.

Influencer marketing is a huge business.[13] It is prevalent on virtually all digital media platforms, and popular influencers often appear on multiple platforms. Social media influencers are extremely popular with children and teens. Many influencers are under age 18, and some are much younger. During the week of May 3, 2021,

for example, 3 of the top-5 most viewed US-based YouTube channels featured child influencers in videos directed to children. For example, the second-ranked *Kids Diana Show* was viewed 379.5 million times.[14] This channel features 7-year old Diana promoting the "Love Diana" lifestyle product line, which includes dolls, hair accessories, jewelry, and beauty products. These videos are available on both YouTube and YouTube Kids despite Google's claims that they do not allow product placement on the YouTube Kids app. One-third of children under the age of eight regularly watch "unboxing" or "product demonstration" videos,[15] where influencers talk excitedly about toys or other products they have be compensated to promote. These videos which often run more than 10-minutes in length are essentially one long ad. Research has found that children are more likely to nag their parents for products—and to throw a tantrum if they say "no"—after watching unboxing videos than after watching traditional television commercials.[16]

In addition to YouTube, other sites popular with children and teens are rife with influencer marketing. On TikTok, well-known brands including Doritos, Burger King, KoolAid and McDonalds, have sponsored TikTok Hashtag Challenges in which users create and upload promotions for their brand. On Instagram, one-third of the most viewed Stories came from brands. An investigation by Public Citizen found that many Instagram influencers popular with young were promoting alcohol, cosmetics, and clothing without disclosing they were compensated for their posts.[17] TikTok and Instagram are among the most popular social media sites with teens and, despite Terms of Service that their sites are for thirteen and up, they are also used by millions of younger children.

In short, regardless of platform, much of the digital content seen by children and teens is marketing products to them in a way that is inherently misleading and unfair. Children deserve the same protections from unfair and manipulative marketing regardless of whether they are consuming media on television, a computer, tablet, or mobile phone. Passage of the KIDS Act would apply the traditional protections for kids against covert, unfair and manipulative advertising to the media that young people use today.

The KIDS Act would also address some other harms to children made possible by digital media. For example, it would prohibit certain "nudging" practices, such as autoplay, automatic notifications, and rewards, that make it hard for children to stop using their devices even when it is in their best interest to do so. And in spending so much time online, children are often exposed to inappropriate content, disinformation, bullying, risky behavior, and sexual exploitation.

III. The FTC should do more to protect children

Congress could also help protect children by giving the FTC the encouragement and resources that it needs to do its job. The Children and Teen Online Privacy Act, for instance, would create a much-needed Division of Youth Privacy and Marketing within the FTC.

I am pleased that in 2020, the FTC initiated an investigation under its Section 6(b) authority that will allow it to better understand the digital advertising ecosystem and how it affects children.[18] This investigation should provide invaluable information for the FTC to assess and improve its existing rules. I also hope that the FTC will share its findings with the public so that it can better understand how personal data is collected and used. In the meantime, it is important that the FTC vigorously enforce its existing policies to protect children.

A. The FTC should bring enforcement actions to prevent unfair and deceptive marketing to children and teens

Under its Section 5 authority to prevent unfair and deceptive acts or practices, the FTC has long issued guidance to advertisers regarding endorsements. The Endorsement Guide generally states that product endorsements must not be deceptive, meaning that the endorsements must be truthful, and any sponsorships must be clearly disclosed to consumers. The FTC has already revised the Enforcement Guide to make clear that these requirements apply when advertisers provide financial or other incentives for social media influencers to promote their products online.[19] Yet, the FTC has brought few enforcement actions for online advertising and none involving social media influencers targeted to those most vulnerable, that is, children. This is the case, despite that fact that in 2015, the Georgetown clinic, acting on behalf of the Campaign for a Commercial-Free Childhood and Center for Digital Democracy, documented numerous videos shown on YouTube Kids in which kid influencers promoted toys and unhealthy food and beverages, and asked the FTC to investigate whether this marketing was unfair or deceptive.[20]

While influencer advertising often fails to disclose its sponsorships, even when provided, disclosure does not prevent children from being misled or taken unfair ad-

vantage of. Often, disclosures are made in ways children can't understand: for example, a small written disclosure appears in the corner of the screen of an unboxing video aimed at preliterate children.[21] But even when sponsorships are disclosed orally in child-friendly language, they are ineffective for young children because they view the child influencers or product spokes-characters online as their friends. Last year, the FTC took a positive step by asking in its endorsement guide review whether children are capable of understanding these disclosures. Research clearly shows that children do not.

In sum, the FTC can and should bring enforcement actions against both high-profile influencers that target children, as well as the companies that use influencers to manipulate young people. It should also update the endorsement guidelines to state clearly that unboxing videos and other form of influencer marketing aimed at children is unfair and deceptive regardless of whether sponsorship is disclosed.

B. The FTC should vigorously enforce the COPPA Rule

The FTC should also enforce the existing COPPA Rule more vigorously. Noncompliance with COPPA is rampant. For instance, studies by Professor Serge Engelman found that thousands of children's apps in the Designed for Families section of the Google Play Store were sharing children's personal information with third parties without getting verified parental consent as required by COPPA. The CCFC and others cited this study in a petition asking the FTC to investigate whether Google Play violated Section 5 of the FTC Act by claiming that these apps were appropriate for children when they did not comply with COPPA.[22] Yet again, the FTC did nothing.

In fact, in the 21 years that the COPPA Rule has been in effect, the FTC has brought only 34 enforcement actions, mostly against smaller companies. All were settled without litigation by consent decrees. Often, settlements merely required the defendant to comply with the law and file periodic reports with the FTC. When the FTC has assessed civil penalties, they have been woefully insufficient to incentivize compliance with COPPA.

To change an ecosystem where noncompliance with a law designed to protect children's is the norm, the FTC must engage in much more rigorous enforcement action. The Commission should both bring more COPPA cases and seek much stiffer penalties so it is no longer in companies' interest to ignore the law.

C. The FTC should hold safe harbors accountable

The FTC has also failed to use the enforcement tools available to it in an effective manner. For example, Section 6502 of COPPA established a "safe harbor" regime intended to incentivize compliance with COPPA. Under this provision, third parties can design a compliance program that meets or exceeds the COPPA protections, apply to the FTC for approval, and if approved, the FTC will deem members that follow the approved guidelines to have complied with COPPA.

Unfortunately, as analysis by both Commissioner Chopra and Professor Egelman shows, COPPA safe harbor programs are not enforcing their guidelines. Instead of incentivizing compliance, safe harbors appear to provide a way for companies to avoid complying simply by paying a safe harbor to certify them. Either the FTC should take steps to ensure that COPPA safe harbors programs are kept up to date and enforced, or it should revoke their approval.[23]

IV. Conclusion

The largely unregulated monetization practices of digital media are both unfair and harmful to young people. Congress could take huge strides towards creating a healthier media environment for children and teens by expanding COPPA's protections to teens and closing some of its loopholes such as the actual knowledge standard. Congress could also protect children from unfair and deceptive marketing and many of the most pernicious design features in digital media by passing the KIDS Act or similar legislation.

I appreciate this opportunity to present these recommendations to the Committee on behalf of CCFC and am happy to answer any questions.

Endnotes

[1] Letter to Mark Zuckerberg, April 15, 2021, *https://commercialfreechildhood.org/wp-content/uploads/2021/04/instagram_letter.pdf.*

[2] I have also published law review articles on marketing to children. *Rethinking Children's Advertising Policies for the Digital Age,* 29 Loy. Cons. L. Rev. 1 (2016); *Restricting the Marketing of Junk Food to Children by Product Placement and Character Selling,* 39 Loyola of Los Angeles L. Rev. 447 (2006).

[3] Victoria Rideout & Michael B. Robb, M. B. (2020), *The Common Sense Census: Media Use by Kids Age Zero to Eight* at 23 (2020) and *The Common Sense census: Media use by Tweens and Teens* (2019).

[4] Parenting Children in the Age of Screens, Pew Research Center, (July 2020).

[5] Joseph Jerome and Ariel Fox Johnson, *AdTech and Kids: Behavioral Ads Need a Time-Out* (2021), *https://d2e111jq13me73.cloudfront.net/sites/default/files/uploads/AdTech%20and%20Kids.pdf.*

[6] Sam Levin, *Facebook Told Advertisers It Can Identify Teens Feeling 'insecure' and 'Worthless,'* The Guardian, May 1, 2017, *https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens.*

[7] Reset Australia, *Profiling Children for Advertising: Facebook's Monetisation of Young Peoples Personal Data,* Apr. 28, 2021, *https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens.*

[8] *Children's YouTube is still churning out blood, suicide and cannibalism,* Wired, Mar. 23, 2018, *https://www.wired.co.uk/article/youtube-for-kids-videos-problems-algorithm-recommend.* The former YouTube engineer Guillaume Chaslot quote continues: "It might sometimes, but if it does it is coincidence. Working at YouTube on recommendations, I felt I was the bad guy in Pinocchio: showing kids a colourful and fun world, but actually turning them into donkeys to maximise revenue."

[9] Raymond Zhong and Sheera Frenkel, *A Third of TikTok's U.S. Users May be 14 or Under, Raising Safety Questions,* NY Times, Aug. 14, 2020, *https://www.nytimes.com/2020/08/14/technology/tiktok-underage-users-ftc.html.*

[10] *See, e.g., McDonald v. Kiloo,* N.D. Cal. No.17-cv-04344-JD, Plaintiffs' Motion for Preliminary Approval of Class Action Settlements, (filed Aug. 5, 2020). This case involved a class action against 16 mobile advertising and app monetization companies, referred to as Software Development Kits ("SDKs"). Plaintiffs alleged that the SDKs embedded code into children's games available on the Google Play Store and the Apple App Store to gather and transmit "persistent identifiers" and personal data for tracking, profiling and ad targeting. McDonald v. Kiloo, 385 F.Supp.3d 1022, 1028 (N.D. Ca. 2019). Most people are not aware that children's apps are often embedded with multiple SDK from companies they likely have never heard of such as AdColony, ChartBoost, inMobi, ironSource, Unity Ads, and Vungle.

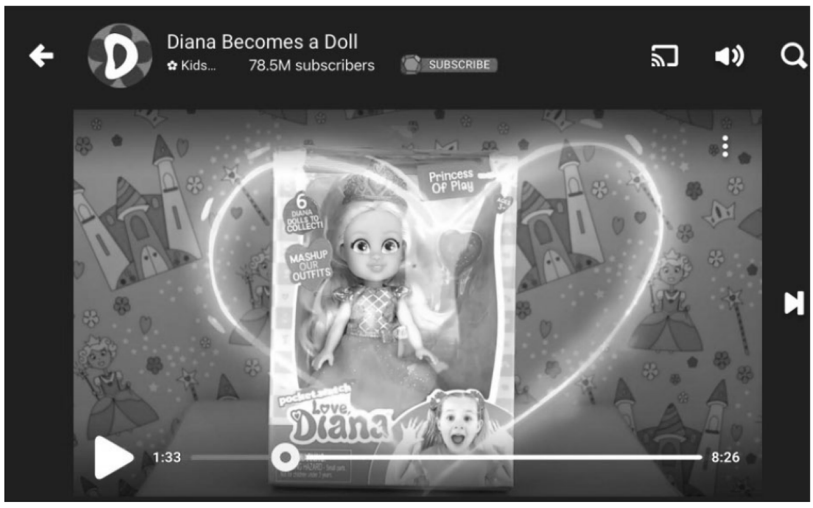
[11] Jenny Radesky, et al, *Digital Advertising to Children,* Pediatrics (July 2020), *https://pediatrics.aappublications.org/content/146/1/e20201681#:~:text=Ban%20all%20commercial%20advertising%20to,eg%2C%20as%20sponsored%20content.*

[12] More than 90 percent of U.S. parents believe COPPA's protections for children should be expanded to teens. *https://parents-together.org/survey-shows-parents-alarmed-as-kids-screen-time-skyrockets-during-covid-19-crisis/.*

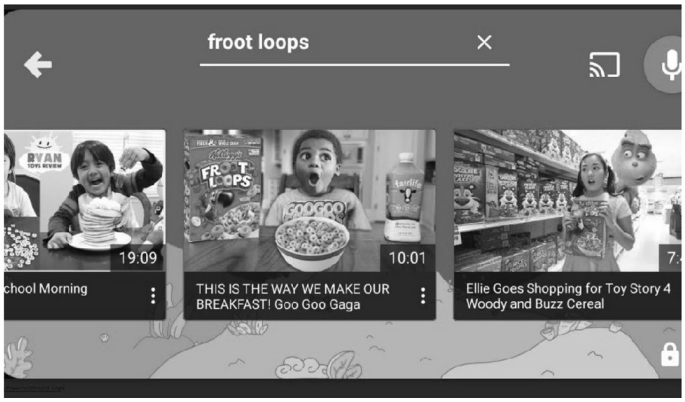
[13] Comments of CCFC and CDD, Guides Concerning the Use of Endorsements and Testimonials in Advertising, FTC Project No. P204500, at 3–15 (June 22, 2020). *https://commercialfreechildhood.org/wp-content/uploads/2020/06/ftc_influencer_comments.pdf.* Recent statistics show that the value of the global influencer market doubled between 2019 and 2021, growing from 6.5 billion to 13.8 billion U.S. dollars in the three years alone. *https://commercialfreechildhood.org/wp-content/uploads/2020/06/ftc_influencer_comments.pdf.* Statistica, *Influencer marketing market size worldwide from 2016 to 2021, https://www.statista.com/statistics/1092819/global-influencer-market-size/.*

[14] Sam Gutelle, Top 50 Most Viewed U.S. YouTube Channels, Week of 05/03/2021, Tubefilter, *https://www.tubefilter.com/2021/05/05/top-50-most-viewed-us-youtube-channels-week-of-05-03-2021.* Child influencers Vlad and Niki had the third largest viewership, and Like Nastya, came in fourth.

Here is are some recent screen shots showing the Kids Diana Show and influencers promoting sugary cereals:



[15] Victoria Rideout & Michael B. Robb, *The Common Sense Census: Media Use by Kids Age Zero to Eight* at 23 (2020). This study also found that 18 percent of all 0- to 8-year-olds follow or subscribe to certain YouTube personalities, celebrities, or influencers, ranging from 4 percent of children under 2, to 16 percent of 2- to 4-year-olds, and 27 percent of all 5- to 8-year-olds. *Id.*



[16] Harsha Gangadharbatla & Deepti H. Khedekar, *The Role of Parental Mediation and Persuasive Knowledge in Children's Consumption of Unboxing Videos Online.* Advertising and Society Quarterly (in press).

[17] Letter to FTC, June 26, 2017, *https://www.citizen.org/wp-content/uploads/migration/case_documents/ftc_instagram_letter_and_investigation.pdf.*

[18] *https://www.ftc.gov/reports/6b-orders-file-special-reports-technology-platform-companies.*

[19] Guides Concerning the Use of Endorsements and Testimonials in Advertising, Request for Public Comment, 85 Fed. Reg. 10105 (2020).

[20] Request for Investigation into Google's Unfair and Deceptive Practices in Connection with its YouTube Kids App, (Apr. 7, 2015); Supplement to Request for Investigation into Google's Unfair and Deceptive Practices in Connection with its YouTube Kids App, (Nov. 24, 2015), Request for Investigation into Violations by Members of the Children's Food and Beverage Advertising Initiative of Pledges Not to Advertise Products to Children that Do Not Meet Uniform Nutrition Criteria, (Nov. 24, 2015); Complaint, Request for Investigation, and Request for Policy Guidance on the Deceptive Practice of Influencer Marketing Directed to Children (Oct. 21, 2016).

[21] Example of a disclosure notice on a video directed to children.

[22] Request to Investigate Google's Unfair and Deceptive Practices in Marketing Apps for Children (Dec. 19, 2018, supplemented Mar. 31, 2021).

[23] See Comments of CCFC, CDD, *et al.,* Request for Public Comment on the FTC's Implementation of the COPPA Rule at 15–21 (Dec. 11, 2019).

Senator BLUMENTHAL. Thanks, Professor Campbell. I am sure that you will have an opportunity to go into those other areas. Mr. Egelman?

STATEMENT OF SERGE EGELMAN, PH.D., RESEARCH DIRECTOR, USABLE SECURITY AND PRIVACY GROUP, INTERNATIONAL COMPUTER SCIENCE INSTITUTE; CTO AND CO-FOUNDER APPCENSUS, INC.

Mr. EGELMAN. Chairman Blumenthal, Ranking Member Blackburn, and distinguished members of this Subcommittee, it is an honor to be here today. Thanks for inviting me.

My name is Serge Egelman, and I direct the Usable Security and Privacy group at the International Computer Science Institute, which is a research institute affiliated with UC, Berkeley. I am also the CTO and co-founder of AppCensus, which is a startup that does privacy analysis of mobile apps.

As background, I have been studying consumer privacy online for almost 20 years now. And actually, over the past 10 years, my research group has focused on mobile apps. And in fact, 2 years ago, and likely the reason I was asked to testify today, was because my lab published a paper where we studied children's apps, specifically. And so, what we did was, we went to the Google Play Store and basically just downloaded as many kids' Android apps as we could. I am picking on Android just because Android is open source and so, we had to write, you know, pretty sophisticated instrumentation into the operating system itself, so that we can monitor exactly what data apps try and access and then, to whom they send it.

Using this instrumentation, we ran almost 6,000 different apps, all, again, targeted at children, self-selected by the developers. When they post those apps into the app stores, it is the app developer who says, you know, this is a child directed app. You know, please list it in the kids' category. And so, given that, that they should all be covered by COPPA.

What we found was that more than half of them had indications that they were likely violating COPPA. So, to give you some examples, about 5 percent of the apps that we looked at transmitted outright contact info like, you know, names, addresses, e-mail addresses, and location data. So, 1 in 20 apps, those are the types of cases that the FTC, you know, has successfully prosecuted in the past.

Forty percent of the apps were transmitting other types of personal information, such as, persistent identifiers, which are used—that is what enables all of this tracking. And I am happy to go into details during questions about how persistent identifiers are used, if you want follow up on that.

Another forty percent of the apps—these are non-mutually exclusive—basically, render the user controllable privacy settings useless. So, on Android and iOS, both Apple and Google offer user controllable settings where you can opt out of tracking. And the way that that works is that, when the user chooses to opt out of tracking, what should happen is that the operating system prevents the apps from accessing, you know, the user resettable identifiers. Or it allows the user to reset those identifiers in much the same way that a user might clear their cookies from the web browser. The

problem is, if they are collected alongside other identifiers, that basically renders that functionality useless. And so, we saw that happening in about 40 percent of the cases.

And then also, you know, to be clear, most of these potential violations that we observed were due to third-party data transfers. So, the apps themselves had, you know, all of these other components. It is very common, in software engineering, to have, you know, third-party components, similar to, you know, other branches of engineering.

So, for instance, a car manufacturer, you know, usually does not make 100 percent of the parts in a car themselves. With software developers will put, you know, prepackaged components in. And the problem comes when those components either are misconfigured by the developer to inadvertently enable tracking of children, despite COPPA-compliant settings that the directors are instructed to use, if the apps that those third-party components are bundled in, are directed to kids. They are supposed to set these settings and that was not happening.

But also, in 20 percent of the apps that we examined, they were sending data to third-parties, whose terms of service explicitly said, "We do not knowingly receive data from children and, therefore, please do not use our components in child-directed apps". Nonetheless, you know, one in five apps appeared to be violating that. And you might wonder why the terms of service has this prohibition. That is because, if you read the privacy policy, you know, for most of these services, they make it pretty clear that the data that is being collected is going to be used for profiling purposes or behavioral ad targeting.

We also found as many Safe Harbor certified apps as we could. So, under COPPA, the FTC has blessed seven organizations as Safe Harbor certifiers. And so, an app developer, or other online service provider, can go to one of these seven services and once, you know, they submit, you know, their product and fill out a questionnaire, the certifier deems the app COPPA compliant and that indemnifies them from FTC action.

So, looking at the Safe Harbor certified apps, we found that they were not appreciably better, in terms of COPPA compliance. And you know, just looking at the raw numbers, they actually appeared to be worse. And that is actually—there is a lot of economics literature on adverse selection with these types of self-regulation programs where it is, you know, the worst actors who have the incentives to participate. You know, the, you know, actors who are already complying with the law, why would they pay money to get certified, you know, to be, you know, against enforcement actions?

So, based on this research, I have four recommendations for improving COPPA. So, one is, you know, the actual versus constructive knowledge standard, and Professor Campbell talked a lot about that. I can go into detail during questions about some of the issues there.

The other problem is the internal operations exemption. So, under COPPA, there is an exemption for collecting, again, the persistent identifiers that enable the tracking ecosystem, if they are collected for internal operations purposes. Which is not exactly defined by statute—in the statute. The FTC in the last round of rule-

making—I think that was in 2013, had added a bunch of categories. The problem is, all of those categories, under internal operations, do not strictly require personal information, you know, to—you know, for those uses. And so, that is why this exemption is kind of moot.

Also, for another reason which is by policy, on the major platforms, both, you know, Google and Apple, they require—Apple for kids apps does not allow developers to collect identifiers, period, for tracking purposes. And so, there is no internal operations exemption that I am aware of, for the Apple platform, if you are an iOS developer. Google has similar policies where collecting persistent identifiers from users requires consent, in many cases. And again, you know, that is why the internal operations exemption, based on my research, it seems to be abused a lot by app developers, partially because they probably do not understand what it means, either. And so, that is why I think that should be eliminated.

The third and fourth thing are related. So, increasing enforcement actions, I have some ideas there. The FTC does excellent work. There are some very smart people there that understand these issues. They are just overburdened. They have, you know, a lot of things on their plate, if they get a lot of complaints to investigate and they just do not have the resources to investigate them all.

And so, finally, you know, in parallel with that, I have some ideas for fixing some of these Safe Harbor programs. One is that it is not clear what they actually do. So, I think, one regulatory update—or I guess, something that the FTC could do through regulation, is set standards and have invited privacy experts to comment and—you know, on the proposed standards that those Safe Harbors should have to follow.

But then, two, the other issue is, my research team had a very hard time identifying what was and was not certified by any of these programs. Many of the apps that we looked at had privacy policies that said they are certified by these programs. Many of the certification organizations had the names of apps on their websites. When the paper was published, many of these organizations said, oh, they have no idea. That it is not actually certified by us, despite the name of the app still appearing on their website for months after, you know, making those public statements.

And so, there is clearly a—you know, I am not going to go and say, you know, bad faith, but there is clearly a lot of consumer confusion here. And so, I think, one fix there is just mandating that every Safe Harbor organization should have to publicly post what apps are actually certified and what versions of those apps. Because any time the software is updated, the privacy behaviors could change and it might—you know, suddenly a software update occurs and now the app is doing something that would violate COPPA, but it has been indemnified due to the Safe Harbor. And so, that is a situation that I think needs to be addressed. And I will leave it at that.

[The prepared statement of Mr. Egelman follows:]

PREPARED STATEMENT OF SERGE EGELMAN, PH.D., RESEARCH DIRECTOR, USABLE SECURITY & PRIVACY GROUP, INTERNATIONAL COMPUTER SCIENCE INSTITUTE; CTO AND CO-FOUNDER APPCENSUS, INC.

Contents

---

1 Introduction and Summary

Chairman Blumenthal, Ranking Member Blackburn, and Distinguished Members of the Subcommittee, thank you for the opportunity to testify today about children's online privacy and the mobile app ecosystem.

My name is Serge Egelman, and I direct the Usable Security and Privacy research group at the International Computer Science Institute, which is a research institute affiliated with the University of California, Berkeley.[1] I hold a PhD from Carnegie Mellon University's School of Computer Science and a BS in computer engineering from the University of Virginia. I am also the CTO and co-founder of AppCensus, which is a startup that builds tools to analyze the privacy behaviors of mobile apps.[2] I also consult for state and Federal regulators on issues pertaining to online consumer privacy and security.

For the past 17 years, I have been studying consumer privacy preferences, how they make online privacy decisions, and how the online ecosystem can be better designed to both protect consumers and help them make more informed decisions. For the past 10 years, I have studied privacy in the mobile app space, including examining what personal information mobile apps are collecting and sharing, and how that might contrast with consumer expectations, laws, and platform policies. Most relevant to the Subcommittee, two years ago my research group published a study of mobile apps' compliance with the Children's Online Privacy Protection Act (COPPA). We used our tools to test 5,855 Android apps that were directed to children and found that more than half appeared to be violating COPPA [3].

My goal through this testimony is to explain how online tracking works, my research on COPPA violations in the mobile app ecosystem, and how the law can be updated to keep pace with rapid technological change to better protect children online. Based on this research, I offer four specific recommendations for improving COPPA:

- *Moving from an "actual" to "constructive" knowledge standard*
- *Eliminating the internal operations exemption*
- *Fixing the Safe Harbor program*
- *Increasing enforcement*

2 Background on Mobile Tracking

To monetize many online services, companies pay those services to show specific advertisements to specific users. They do this by inferring individual users' preferences based on data automatically collected from them: the services they use, how

---

[1] *https://www.icsi.berkeley.edu/*
[2] *https://www.appcensus.io/*

they use them, from where they use them, and so forth. In short, online and offline activities are tracked, which allows companies to maintain detailed profiles of individual user behavior, which in turn is used to predict users' interests, preferences, and even demographics. The collected information may be used to predict a consumer's religion, health conditions, sexual orientation, or political affiliation; some of this information may be revealed by the phone's GPS location alone, or even by just the name of the app that is being used.

In most cases, this data is used to target advertisements, but in some cases it is sold to data brokers, who use it to augment profiles of the same consumers that they collected from other sources, and then sell it to whoever is willing to pay for it. Obviously, this is even more concerning when the data comes from children, who are unlikely to understand that this is happening, much less consent to it, but who could potentially face enormous impacts due to future usage of this data. This data may be used for manipulative marketing campaigns, but also may feed biased and unaccountable algorithms that use it to make decisions about a child's future, not to mention outright malicious uses of the data.

Contrary to popular belief, the reason why you receive oddly prescient ads is not because your devices are secretly recording your conversations, but because of this type of inference: your online and offline activities are tracked, and then sophisticated algorithms use that data to make predictions about you. Tracking is made possible by "persistent identifiers." An identifier is any piece of information that allows an individual—or device—to be uniquely identified. "Persistent" identifiers are identifiers that tend to not change over time. For example, motor vehicles have persistent identifiers in the form of license plates: a license plate uniquely identifies a vehicle and vehicles tend to have the same license plates over time. Thus, if someone records all the license plates at a particular place over time, they can determine how many times in that period any individual vehicle was there. Similarly, if license plates are recorded at many different locations and that data is combined into a single dataset, one could use that to reconstruct the movements of individual vehicles in that dataset. As can be seen, combining a persistent identifier with information about where that identifier was observed allows a data recipient to reconstruct an individual's activities. Using this knowledge, one could infer information about their routines, preferences, demographics, and even relations and social connections!

While this type of mass surveillance may seem appealing to some for the increased security they believe it may enable, a wealth of scholarship exists to show why this is a false tradeoff (e.g., [4, 5]).

This is precisely how mobile tracking occurs. Mobile phones have various identifiers associated with them, including some that cannot be easily changed (*e.g.,* serial number, WiFi MAC address, IMEI, etc.). As mobile phones are very personal devices, a unique identifier for a mobile phone is consequently a unique identifier for that individual and can therefore be used to collect data about their activities, preferences, and demographics, simply based on data collection that associates it with the apps that were used, when, how, and where.

Why does this matter? By and large, this data is used for advertising purposes: these profiles are used to decide which ads to show which users, allowing advertisers to target individuals based on their inferred interests and preferences. However, the data is increasingly used for other purposes that are often completely opaque to consumers, particularly parents. For example, location data collected by apps is frequently resold to other businesses and used for everything from predicting social relations in the physical world, to predicting retail sales trends, for law enforcement surveillance, and even for political fundraising and advocacy. This data is being collected without consumers' knowledge, and then is misused in ways that undermine individual rights. Worse, new uses for this type of data are invented all the time, which means that there's no way of knowing exactly how collected data may be used in the future. Data collected from mobile apps and other services could end up being used for making major life decisions, such as whether offers of credit or employment are extended, or whether someone is admitted to a particular school, or even the type of medical care that they may receive. When this data comes from children, it is obviously even more concerning.

3 Research Findings

As part of prior research to study how mobile apps' privacy practices comport with consumers' expectations, my lab wrote bespoke instrumentation for the Android platform that allows us to run mobile apps and monitor exactly what personal data those apps access and to whom they transmit it [6, 7, 8, 2]. We wrote our tools for Google's Android platform only because it is open source: having the source code for the operating system allowed us to modify it for this purpose; at the time, we didn't

look at Apple's iOS simply because we didn't have the source code to add the same level of instrumentation.

Starting in late 2016, we began downloading as many free apps in the "Designed for Families" (DFF) program as we could find, which ended up being just under 6,000 apps [3]. The DFF program is a section of the Play Store, Google's centralized Android app market, which is exclusively for apps that are directed to children. Mobile app developers must participate in the program when they upload their app and disclose to Google that it is directed at children. As part of the program, they must affirm to Google that their app is in compliance with COPPA. Our goal was to evaluate whether that was the case in practice.

3.1 Collection of Contact and Location Information

In terms of the most serious privacy violations, we observed that roughly 300 of the apps that we tested (4.8 percent) were collecting children's contact information (*e.g.,* names, e-mail addresses, and phone numbers) and/or precise location data, which included apps specifically targeted at children under 5. In most cases, this data was transmitted to third-party advertising companies, or third parties that otherwise support the advertising industry. I believe that this is a serious finding that should be put in perspective: roughly 1 in 20 of the apps that we examined were collecting information without the requisite verifiable parental consent, and for which the FTC has previously brought cases.

3.2 Insecure Transfer of Personal Information

The most common issue that we observed was the transmission of personal data using insecure means. Under COPPA, covered services are required to "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[3] While neither the statute nor regulations define what are considered "reasonable procedures," Transport Layer Security (TLS) and its predecessor have been industry standards for more than three decades now; its use is required on U.S. government websites.[4] Simply put, it is not considered "reasonable" to transmit personal information without the use of TLS to secure it. Nonetheless, we observed that 40 percent of the children's apps (2,344 apps) we tested failed to take this reasonable procedure.

What this means is that for users of these apps, their personal information is accessible to any eavesdroppers. This may include anyone sharing the same WiFi connection, as well as Internet service providers and other organizations. In an extreme case, this could enable someone to identify a specific child within a specific area, based on the insecure transmissions emanating from that child's device.

3.3 Targeted Advertising

The remaining pervasive privacy issues that we discovered had to do with the collection of persistent identifiers. A persistent identifier is simply a label that is unique to an individual, such as a Social Security Number or the serial number of a personal device. While a persistent identifier might appear as an insignificant random number or combination of letters, as I explained, persistent identifiers are primarily what enable targeted advertising and other types of data collection. We identified multiple issues, including: (1) Google's user privacy settings may fail to work due lack of policy enforcement and (2) many app developers fail to correctly configure third-party software components to limit data collection from children, resulting in children's personal information being sent to third parties for targeted advertising and other purposes.

3.3.1 Ineffective Android Privacy Settings

Prior to 2013, mobile apps for both Google's Android and Apple's iOS mobile operating systems collected a variety of different non-resettable identifiers that were used to track consumers. Unlike cookies in the web browser, which can be periodically cleared by the user, many of these identifiers cannot be reset, and so mobile device users had neither transparency into who was tracking them nor when they were being tracked, nor any control over it. In response, both Apple and Google created software-based "advertising identifiers" that could be reset through user-facing privacy controls. By policy, both platforms mandate that only these identifiers be used to track users, in lieu of other non-resettable identifiers. This is so that a consumer can opt out of tracking via the provided settings interface. However, as we discovered on Android, compliance with this policy is not enforced by Google: app developers and the third-party mobile SDKs embedded within their apps are able to collect other non-resettable identifiers alongside the advertising ID. When this

[3] 15 U.S.C. § 6502(b)(2)(D)
[4] *https://https.cio.gov/*

happens, if a consumer resets their advertising ID or uses the privacy settings interface to opt out of tracking altogether, data recipients are simply on their honor to stop tracking that consumer.

We observed that 39 percent of the children's apps that we tested transmitted non-resettable identifiers alongside the user-resettable advertising ID. What this means is that for users of these 2,281 apps, Google's ad privacy settings may simply be ignored.

3.3.2 Ineffective SDK Privacy Settings

Software engineering, like many other types of engineering, involves building products out of many pre-made components. For example, just as a car manufacturer does not make all the components in its cars (*e.g.,* springs and shocks may come from other manufacturers, sheet metal is purchased from suppliers, etc.), a mobile app developer does not necessarily write all of the code found within their apps. Third-party software development kits (SDKs) allow developers to include pre-made software components, saving them time and effort. For example, rather than find advertisers, organize and/or create ad copy, and then determine which users to show which ads, app developers can simply outsource that work by incorporating a third-party ad SDK that has already implemented those things. There are third-party SDKs that help developers with displaying graphics, processing payments, streaming audio or video, and so forth. This type of "code reuse" is an accepted part of modern software engineering. However, it creates enormous risks, especially when app developers fail to verify that third-party components are functioning as expected (or if third-party components are misused).

Many of the potential COPPA violations that we observed were due to the data collection behaviors of third-party SDKs, and not necessarily due to code written by app developers; nonetheless, most apps embed these third-party SDKs, and therefore they impact a lot of apps. Many of these SDKs, because they are for use in a wide variety of mobile apps, offer app developers configuration options so that they can be customized to an app's needs. Specifically, many of the SDKs that collect personal data with COPPA implications—those that may be used to collect personal information from children—offer developers configuration options to enable a COPPA-compliant data-collection mode. When the app developer uses one of these directives to signal that the user is a child, the SDK is instructed to either not use that child's personal information for COPPA-prohibited purposes or to not send that data to its servers altogether. When developers of children's apps fail to correctly configure these types of options, it likely results in children's personal data being collected for targeted advertising and other prohibited purposes.

We observed that few developers were correctly configuring third-party advertising SDKs to disable the collection of personal information for profiling and/or ad targeting purposes. For example, we observed that 1,280 of the children's apps we tested (21.9 percent) transmitted users' personal information to Facebook's servers. Of these, only 75 (5.9 percent) correctly signaled to Facebook that the user is a child and that the data should be handled pursuant to COPPA. However, Facebook is not an isolated example: of the third-party SDKs that we observed collecting personal information and that offered options for child-directed treatment, none were consistently configured correctly by app developers.

Other third-party SDKs simply provide terms of service that prohibit their use in child-directed apps. However, we observed that developers of children's apps use these SDKs anyway. By reading the terms of service and privacy policies of these data recipients, my research team identified several data recipients who (1) describe using data received from their SDKs for practices that would be prohibited by COPPA, if that data were to come from children; and (2) prohibit inclusion of their SDKs in child-directed apps and disclaim any knowledge of receiving data from children. Despite this, we identified 1,100 children's apps transmitting personal information to these companies (18.8 percent of the children's apps we tested).

4 Recommendations for Fixing COPPA

Based on my research, which exposed evidence of rampant non-compliance with COPPA's existing requirements, I have several recommendations for strengthening COPPA, which I detail in this section:

- *Moving from an "actual" to "constructive" knowledge standard*
- *Eliminating the internal operations exemption*
- *Fixing the Safe Harbor program*
- *Increasing enforcement*

4.1 Moving from "Actual" to "Constructive" Knowledge

Many of the potential violations that we observed amounted to sharing of persistent identifiers—without verifiable parental consent—with companies whose privacy policies state that those identifiers will be used for user profiling and/or behavioral advertising, activities that are prohibited by COPPA (when that data comes from children). These persistent identifiers are generally collected and transmitted by third-party SDKs, and so it is plausible that many app developers simply do not know when this data is being transmitted. However, the third-party data recipients know, and in most cases, the information that they are currently receiving allows them to trivially determine that the transmitting app was directed at children.

The privacy policies of many of the companies that receive personal information from children's apps state they are directed at general audiences and have "no actual knowledge" of receiving personal information from children, thereby absolving them of any responsibility under COPPA. This, however, ignores the fact that each transmission from an SDK usually includes the name of the app that transmitted the data. The claim that a third-party data recipient does not have actual knowledge relies on not knowing whether a particular app is targeted at children. Yet, when one looks at the marketing materials of the companies receiving this data, and their business models, it is apparent that this is precisely the type of knowledge that they claim to possess!

Many online advertising business models rely on knowing the demographics of specific apps so that they can target ads based on those demographics. That is, their internal data allow them to already know or trivially find out which apps are child-directed. For data recipients who genuinely do not maintain that data, they can simply query the Google Play Store to determine whether or not a given app is in the Designed for Families program (and therefore targeted at children) based on its public metadata. I can personally write and test the code to do this in under an hour. There are also many commercial offerings that offer companies programmatic access to this type of data. But despite the ease with which data recipients *could* automatically determine whether or not they are receiving data from a child-directed app, they choose not to. Instead, most developers of third-party SDKs place the burden on app developers, rather than using the information that is likely already in their possession—or trivially available to them—to automatically configure their services for COPPA compliance.

As I have observed in the course of my research, many app developers configure these settings incorrectly (or are simply unaware that such settings exist), which results in children being tracked and profiled. If third-party data recipients are held to a "constructive knowledge" standard, under which they would be required to use the information at their disposal to identify whether the data they receive originates from child-directed services, this would not only result in greater compliance and reduced harm to children, but it would also result in drastic cost savings, especially amongst smaller software development companies and individual entrepreneurs. One ad network using their existing data—or data reasonably available to them—to automatically apply child-directed treatment to the data they receive would negate the need for app developers to individually spend time and effort to correctly configure that company's SDK to do so. More to the point, a constructive knowledge standard would shift the burden of compliance away from millions of small app developers—who would still need to report whether or not their apps and services are child-directed—to the significantly fewer number of data recipients, who are much better positioned to apply privacy protections to the data that they collect (and are much more likely to do so correctly). In sum, my research and experience suggest that moving to a constructive knowledge standard would result in fewer incidents of children being inadvertently tracked and profiled, as well as economic savings to businesses by lessening their compliance costs.

4.2 Eliminating the Internal Operations Exemption

Currently, persistent identifiers can be collected from children without parental con-sent if they are used for the site or service's "internal operations," which are currently defined by regulations as using the data to:[5]

1. Maintain or analyze the functioning of the Website or online service;
2. Perform network communications;
3. Authenticate users of, or personalize the content on, the Website or online service;

[5] 16 C.F.R. § 312.2

4. Serve contextual advertising on the Website or online service or cap the frequency of advertising;
5. Protect the security or integrity of the user, Website, or online service;
6. Ensure legal or regulatory compliance; or
7. Fulfill a request of a child as permitted by § 312.5(c)(3) and (4);

From a technical standpoint, the collection of persistent identifiers that allow a user's activities to be tracked between apps is unnecessary for any of these purposes. The primary issue is that each of these use cases could be facilitated by an identifier that is unique to a session, an app installation, or developer, which in turn could not be used to track the user across other apps and services. For example, serving a contextual ad simply requires knowing the type of app or website that a user is using or visiting, which is information that is already collected; by definition, contextual ads are based on those things alone and *not* the user's identity, and therefore do not require the collection of persistent identifiers. Similarly, conversion tracking, measurement, fraud detection, and advertising attribution also do not need persistent identifiers that can identify users across apps. If they are not performing COPPA-prohibited profiling and behavioral advertising, an advertising company only needs to know *how many* people clicked on a specific ad, not *who* those individuals are. When user-specific identifiers are needed, ephemeral app-specific or session-specific identifiers can be used. This functionality is already supported on both Android and iOS, and therefore eliminating the internal operations exemption should not create an undue compliance burden.

Furthermore, claims that persistent identifiers are needed for these purposes are disingenuous because many app developers are already prevented by platform policies from using identifiers for many of these purposes. Indeed, on iOS, if a user opts out of online tracking, apps are outright prevented from accessing identifiers that could be used to track that user's behaviors across apps. Further, Apple already requires that *no* persistent identifiers can be collected from children's apps.[6] Google provides best practices for developers that explain how ephemeral identifiers can be used for many of these use cases to preserve user privacy.[7] Thus, it is patently false to claim that persistent identifiers are necessary for these purposes.

The FTC has previously advocated for companies to take a "data minimization" approach to online privacy.[8] I recommend that the Subcommittee heed this advice with regard to children's privacy: because long-term persistent identifiers are unnecessary for these purposes, the internal operations exemption should be eliminated from COPPA.

4.3 Fixing the Safe Harbor Program

The FTC is charged with certifying Safe Harbor self-regulation programs under COPPA. As of this date, the FTC's website indicates that seven such programs are currently certified.[9] In the course of my group's research [3], we identified 237 Android apps that gave outward appearances of having been certified as COPPA-compliant by these programs. Yet, when we examined their behaviors, we observed that 24 (10 percent) collected location data and/or contact information without verifiable parental consent, while 77 (32 percent) transmitted personal information without taking "reasonable" security precautions (*e.g.,* using TLS encryption). We concluded that apps certified by these programs were just as likely to comply with COPPA as apps not certified by them. Indeed, this finding is consistent with prior research on industry self-regulation, which found that websites receiving trust certifications "are more than twice as likely to be untrustworthy as uncertified sites" [1]. This begs the question, if an organization is already complying with the law, why would they spend additional money to protect themselves from enforcement of that law?

Given the poor incentive structures and lack of transparency into how apps are being certified or even determining *which* apps are certified, current Safe Harbor programs do not appear to be effective. I have three suggestions for improvements that can be made:

1. *Apps and services should be certified only after independent forensic evaluations of their privacy behaviors.*
2. *The FTC should develop, in consultation with privacy experts, standards for forensic evaluations of mobile apps' privacy behaviors.*

---

[6] *https://developer.apple.com/app-store/review/guidelines/#kids-category*
[7] *https://developer.android.com/training/articles/user-data-ids*
[8] *https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices*
[9] *https://www.ftc.gov/safe-harbor-program*

3. *Certification organizations should publish lists of the apps that they have certified (including versions).*

Based on my examination of the public documents that describe COPPA Safe Harbor certification processes, it appears as though current certification processes rely primarily on self-reports from app developers, rather than forensic examinations of their apps (that would yield the type of data that is necessary to assess compliance). Given that many app developers are unaware of the privacy issues associated with their apps, it would hardly be a surprise that those behaviors do not get disclosed to the certification organizations, resulting in COPPA-violative apps inadvertently being certified.

Relatedly, one of the hardest parts of my analysis was simply finding the apps that had been certified by each organization, as many did not publish information about how they certified each app nor what specific apps or versions were even certified. Instead, we relied on press releases from those companies, as well as images and text on their websites and references in the privacy policies of individual apps. Upon publication of these findings, many Safe Harbor organizations claimed that the apps that we examined were not actually certified by their organizations (despite their names and logos appearing on each other's websites). Given that a team of multiple PhDs and a lawyer could not disambiguate what has and has not been certified by each program, it is hard to expect the average parent to be able to. Thus, by mandating that this information be public and in an accessible manner, not only would it empower parents to make better decisions, but it would strengthen the free market through increased transparency, thereby promoting competition.

4.4 Increasing Enforcement Efforts

Finally, all of the above changes are moot without increased enforcement efforts. In under a year of work, my research lab identified the transmission of personal information for tracking and advertising purposes from literally thousands of child-directed mobile apps. At the same time, the FTC, the primary entity empowered with enforcing COPPA, historically has pursued only 1–2 COPPA enforcement actions each year. This is not for want of known violations. To be clear, the FTC employs very capable attorneys and technologists who do excellent work. The problem is that there simply are not enough of them to investigate all of the violations brought to their attention. As the primary agency tasked with enforcing COPPA, it is my opinion that the FTC does not have enough resources to bring enough cases for the threat of enforcement to serve as a deterrent; similar resourcing problems appear to prevent state attorneys general from filling this enforcement vacuum. Simply put, if the FTC continues to not receive funding commensurate with its enforcement responsibilities, COPPA will remain another unfunded mandate.

I strongly believe that the enforcement problems can be addressed in two complementary ways. First, the FTC needs a significant increase to its privacy enforcement budget. However, unless this budget is increased by orders of magnitude, it is still unlikely to be enough for them to be able to investigate all of the potential violations brought to their attention. That is why I believe that as a second recommendation, Congress should look to the free market and create a private right of action. With a private right of action, market forces will drive compliance, while at the same time, they will also drive competition among industry self-regulation programs. These industry self-regulation programs can then be better regulated by the FTC to ensure that they are accurate and transparent.

5 Conclusion

My research has shown that despite COPPA, mobile apps directed at children frequently collect children's personal information and share it with third-party advertisers and data brokers. I believe that many of the problems that I've outline in this testimony can be addressed through changes to COPPA. I believe that these proposed changes will result in greater levels of compliance amongst online services, in-creased transparency for parents, better protections for their children, and increased competition in the marketplace.

Thank you for giving me the opportunity to testify today. Please do not hesitate to follow up with me regarding any questions that you may have.

References

[1] B. Edelman. Adverse selection in online 'trust' certifications. In *Proceedings of the 2006 Workshop on the Economics of Information Security (WEIS'06),* Cambridge, UK, 2006.

[2] J. Reardon, A. Feal, P. Wijesekera, A. E. B. On, N. Vallina-Rodriguez, and S. Egelman. 50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System. In *Proceedings of the 24th USENIX Security Symposium,* USENIX Security '19, Berkeley, CA, USA, 2019. USENIX Association.

[3] I. Reyes, P. Wijesekera, J. Reardon, A. E. B. On, A. Razaghpanah, N. Vallina-Rodriguez, and S. Egelman. "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. *Proceedings on Privacy Enhancing Technologies,* (2018.3):63–83, 2018.

[4] D. J. Solove. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review,* 44, 2007. *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565.*

[5] D. J. Solove. Why Privacy Matters Even if You Have 'Nothing to Hide'. *The Chronicle of Higher Education,* May 15 2011. *https://www.chronicle.com/article/why-privacy-matters-even-if-you-have-nothing-to-hide/.*

[6] P. Wijesekera, A. Baokar, A. Hosseini, S. Egelman, D. Wagner, and K. Beznosov. Android permissions remystified: A field study on contextual integrity. In *24th USENIX Security Symposium (USENIX Security 15),* pages 499–514, Washington, D.C., Aug. 2015. USENIX Association.

[7] P. Wijesekera, A. Baokar, L. Tsai, J. Reardon, S. Egelman, D. Wagner, and K. Beznosov. The feasability of dynamically granted permissions: aligning mobile privacy with user preferences. In *Proceedings of the 2017 IEEE Symposium on Security and Privacy,* Oakland '17. IEEE Computer Society, 2017.

[8] P. Wijesekera, J. Reardon, I. Reyes, L. Tsai, J.-W. Chen, N. Good, D. Wagner, K. Beznosov, and S. Egelman. Contextualizing privacy decisions for better prediction (and protection). In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems,* CHI '18, pages 1–13, New York, NY, USA, 2018. Association for Computing Machinery.

Senator BLUMENTHAL. Thank you very much, excellent. Baroness Kidron, I hope we have you remotely.

STATEMENT OF BARONESS BEEBAN KIDRON, OBE, CROSSBENCH PEER, HOUSE OF LORDS, UK; CHAIR, 5RIGHTS FOUNDATION

Ms. KIDRON. You do, indeed. And thank you, Chairman Blumenthal and Ranking Member Blackburn for inviting me to address this critical issue. My apologies for not being with you in person.

I think it is important to make explicit that while I am a member of the House of Lords, I am not a member of a political party nor the government, but I sit as a crossbench peer. This affords me the great privilege of working across both Houses on a truly nonpartisan basis. And I have authored and introduced legislation on this subject and participated in several committee inquiries. I am the Co-Founder and Deputy Chair of the All-Party Parliamentary Group for Digital Regulation and Responsibility. And outside parliament, I chair the 5Rights Foundation, a charity that is dedicating to build—to building the digital world young people deserve.

In 2018, as part of the Data Protection Bill, I introduced an amendment to create the "Age-Appropriate Design Code". The AADC, or the Children's Code, as it is fondly and commonly known, has some key features. The Code defines a child as any person under the age of 18. This is in stark contrast with the tech sector that has exploited a gap in legislation to treat all 13-year-olds as adults, when any parent will tell you that their 13-year-old is not yet an adult. Similarly, the Code is applicable to services likely to be accessed by children, rather than restricting protections to services directed at children. Most children spend most of their time online on services which are primarily designed for adult use.

The 15 provisions of the Code offer children a high bar of data protection, including protections from revealing their location, using a child's personal data to deliver detrimental material, or deliberately nudging them to give up their privacy. And as the September 2 deadline for compliance approaches, the impact of this one small legislative effort is becoming apparent as companies have to redesign their services to better protect minors.

In a recent conversation with one of the major platforms, I was told that all their product teams now have to consider not only the 15 provisions in total, but also really interrogate what its overarching requirement, to process children's data in, I quote, "the best interest of children". And if I might actually quote the code directly, it states, "It is unlikely that the commercial interest of an organization will outweigh a child's right to privacy".

These baseline protections are overwhelmingly popular with the public, that is a public tired with industry norms that promote intrusive and addictive design practices or exacerbate and recommend harmful material. And they are, frankly, sickened by the idea that a child's real time location can be tracked by a stranger or predator.

Four years ago, the UK government announced that they would make the UK the safest place to be online by introducing an Online Harms Bill. Last week, they finally published the text of that bill as the Online Safety Bill. This change of title is an important reflection of the journey government officials have been on. It is now widely accepted that we cannot argue over what is and is not acceptable only after gross harms have been committed, after children have suffered. We must consider their safety in advance.

We cannot allow commercial interests to target a depressed or unhappy teenager on a Friday night with ads for inappropriate drugs, expose 9-year-olds to explicit interactions with adults, or push dangerous challenges to children through algorithmic recommendations. Just a month ago, a 12-year-old from Colorado died after taking part in a blackout challenge that was viral on a video-sharing app.

Mr. Chairman, I know that you are a premier advocate for Consumer Education. And as I have worked on this issue around the world, gradually policymakers have come on board. But still parents, teachers, and very often children themselves feel helpless to understand how they are being manipulated. At 5Rights, we are about to launch a campaign to help bridge this gap. It is called Twisted Toys and we have built a suite of toys that manifest in a palpable way how Big Tech is spying on and putting children at risk. This disturbing project graphically illustrates the urgent need for action, and I hope you will be seeing a lot more about it in the next month or two.

We do not accept this manipulation of children anywhere else. We must not accept it online. And the reason that parents, teachers, and children feel overwhelmed that this is—is because this is not a problem that parents, teachers, or kids can solve on their own. A system designed to extract every ounce of a child's attention, expose them to an infinite public, and encourages them to get lost in the mirror of anxiety, is simply not healthy. The tech sector has the ability to raise the ceiling and give children back their childhood. But it is up to lawmakers to insist on the floor of behavior below which they must not go.

And while the Children Code arguably makes UK's children online safety standards the highest in the world, it simply will not be good enough. The deficit in American standard setting on these issues is alarming. The U.S. is home to the most influential tech companies in the world. We are doing what we can to protect our

children, but we do need this administration and we do hope you will act. Because the norms you establish in the U.S. impact on every connected child in the planet, and that is nearly 1 billion children and counting.

I look forward to your questions.

[The prepared statement of Ms. Kidron follows:]

PREPARED STATEMENT OF BARONESS BEEBAN KIDRON, OBE, CROSSBENCH PEER, HOUSE OF LORDS, UK; CHAIR, 5RIGHTS FOUNDATION

Thank you, Chairman Blumenthal and Ranking Member Blackburn for inviting me to address this critical issue. I am devoted to protecting children from online harms and hope that my legislative experience in the United Kingdom and my work with other countries might be of some benefit to this Committee. I understand you are considering how to better protect children from the dangers they face online every day. Children are being monetized by the digital products and services focused on the relentless pursuit of every ounce of their attention and data, putting them at grave risk of harm.

It is important to make explicit that while I am a member of the House of Lords, I am not a member of a political party nor the government but sit as a crossbench peer. This position affords me the great privilege of working across both Houses on a truly non-partisan basis. I have authored and introduced legislation on this subject and participated in several committee inquiries. I am co-founder and deputy chair of the All-Party Parliamentary Group for Digital Regulation and Responsibility. Outside parliament, I chair the 5Rights Foundation,[1] a charity that does ground-breaking work around the world to make systemic changes to digital systems in order to protect children. 5Rights developed a Child Online Protection Policy for the Government of Rwanda, has supported multiple nation state efforts to develop data protection regimes, and is working in partnership with the Institute for Electrical and Electronics Engineers (IEEE) to co-create Universal Standards for Children and for Digital Services and Products. Most recently, 5Rights supported the Committee on the Rights of the Child (UNCRC) in drafting general comment No. 25 (2021) on children's rights in relation to the digital environment.[2] This authoritative document adopted in March this year is anticipated to have global significance on the expectations and duties of states and business to children. I also work with international bodies such as the Organization for Economic Cooperation and Development (OECD), UNESCO Broadband Commission and EU organisations on issues such as Artificial Intelligence (AI), child-centred design and data protection.

In 2012, when smartphones began to be priced at a point that allowed a parent to provide this powerful device to a child, childhood fundamentally changed. This device, increasingly glued to their pocket, bedroom, hand, and gaze, gave children unfettered access to a world of breath-taking richness and variety. It also gave adults and commercial entities unfettered and unchecked access to children—access that has been ruthlessly exploited.

In the UK, it has been 150 years since we took children out of the chimneys and put them in the classroom—arguably the beginning of what we now conceive of as childhood. Childhood is a journey from dependence to autonomy with its own set of vulnerabilities and learning. Childhood is not a risk-free business, but there is broad consensus that we have a duty of care, which requires us to protect children from foreseeable risks and preventable harms—a duty on us as parents, politicians and businesses. This consensus is taken for granted in the decisions we make about all parts of children's lives—except the digital world. Members of this committee that is not acceptable. My personal battle and political commitment is to ensure this wrong is put right.

In 2018, as part of the Data Protection Bill, I introduced an amendment to create the "Age Appropriate Design Code (AADC).[3] The AADC, or Children's Code, as it is commonly known, has some key features. The Code defines a child as any person under the age of 18. This is in stark contrast with the tech sector that has exploited a gap in legislation to treat all 13-year-olds as adults, when any parent will tell you

[1] *https://5rightsfoundation.com/*

[2] *https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2fC%2fGC%2f25&Lang=en*

[3] *https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/*

that their 13-year-old is not an adult. Similarly, the Code is applicable to services 'likely to be accessed by children' rather than restricting protections to services directed at children. Most children spend most of their time online on services which are primarily designed for adults.

The 15 provisions of the Children's Code are interconnected and interdependent—but together they offer children a high bar of data protection, including protections from revealing their location, using a child's personal data to deliver detrimental material, or deliberately nudging them to give up their privacy. As the September 2nd deadline for compliance approaches, the impact of this one small legislative effort is becoming apparent as companies have to redesign their services to better protect minors, including disabling features that allow direct messaging of children by unknown adults,[4] providing clearer terms of service,[5] putting age assurance schemes in place,[6] offering tailored services for children of different ages,[7] and making default settings that automatically offer a high bar of safety and data privacy for children's profiles.[8]

The full impact of the Children's Code remains to be seen, but in a recent conversation with one of the major platforms, I was told that all their product teams now have to consider the Code's 15 provisions, including its overarching requirement to process children's data in "the best interests of children", and if I might quote the Code directly, which states that: "It is unlikely that the commercial interests of an organisation will outweigh a child's right to privacy."[9] These baseline protections are overwhelmingly popular with the public that is tired of industry norms that promote intrusive and addictive design practices, or exacerbate and recommend harmful material, and they are sickened by the idea that a child's real time location can be tracked by a stranger—or predator.

Four years ago, the UK government announced that they would make the UK the safest place to be online by introducing an Online Harms Bill.[10] Last week they finally published the bill itself[11] as the Online ***Safety*** Bill. This change of title is an important reflection of the journey government officials have been on. It is now widely accepted that we cannot argue over what is and isn't acceptable only *after* gross harms have been committed, *after* children have suffered. While those of us in the UK parliament will inevitably scrutinise every line of its 145 pages, its premise—that we all have a duty of care to children, and in the case of digital services, there are design and commercial practises that simply must be off limits—is powerful. We cannot allow commercial interests to target a depressed or unhappy teenager[12] on Friday night with ads for inappropriate drugs, expose 9-year-olds[13] to explicit interactions with adults, or push dangerous 'challenges' to children through algorithmic recommendations. Just a month ago, a 12-year-old from Colorado died after taking part in a "blackout challenge"[14] that was viral on a video-sharing app.

Even with this draft Online Safety Bill, much work remains. In a busy legislative season, I will also be introducing a private member's bill to set standards for age assurance providers. While private member's bills rarely end up as statutes, they are an important vehicle for policy makers to flesh out arguments. Every policy conversation about children in the digital world eventually comes down to the question of age assurance and age verification. I have shared a recent 5Rights report[15] "*But how do they know it is a child*?" with the Subcommittee as part of my written testimony. Age assurance is a not a question of innovation, but of governance and agreed standards. Since the release of "*But how do they know it is a child*?" and the an-

---

[4] *https://about.instagram.com/blog/announcements/continuing-to-make-instagram-safer-for-the-youngest-members-of-our-community*

[5] *https://about.fb.com/news/2020/02/messenger-kids-controls/*

[6] *https://blog.youtube/news-and-events/using-technology-more-consistently-apply-age-restrictions/*

[7] *https://blog.youtube/news-and-events/supervised-experiences-for-families-on-youtube/*

[8] *https://blogs.windows.com/windowsexperience/2021/04/15/introducing-microsoft-edge-kids-mode-a-safer-space-for-your-child-to-discover-the-web/*

[9] *https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/1-best-interests-of-the-child/*

[10] *https://www.gov.uk/government/news/making-britain-the-safest-place-in-the-world-to-be-online*

[11] *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf*

[12] *https://www.vice.com/en/article/pg7d59/when-facebook-and-instagram-thinks-youre-depressed*

[13] *https://info.thorn.org/hubfs/Research/Responding_to_Online_Threats_2021-Full-Report.pdf?utm_campaign=H2D_report&utm_source=website*

[14] *https://www.today.com/parents/boy-dies-after-trying-tiktok-blackout-challenge-t215253*

[15] *https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf*

nouncement of my private member's bill, I have been inundated by politicians, businesses, the tech sector, regulators and advocacy organizations, all saying how much they would welcome clear and enforceable standards of practice.

Mr. Chairman, I know that you are a premier advocate for Consumer Education having spent so much of your career as your state's top law enforcement official, so let me finish with one last observation—that has had a surprising outcome. As I have worked on this issue around the world gradually policymakers have come on board—but still parents, teachers and very often children themselves feel helpless to understand how they are being manipulated. At 5Rights we are about to launch a campaign to help bridge this gap. It is called Twisted Toys and we have built a suite of toys that manifest in a palpable way how Big Tech is spying on and putting children at risk. This disturbing project graphically illustrates the urgent need for action—and you'll be seeing more about it in the next month or two.

We do not accept this manipulation of children anywhere else—we must not accept it online. The reason that parents, teachers and children feel overwhelmed is that this is not a problem that parents, teachers or kids can solve on their own. A system designed to extract every ounce of a child's attention, expose them to an infinite public and encourages them to get lost in the mirror of anxiety, is not healthy. The tech sector has the ability to raise the ceiling and to give children back their childhood—but it is up to legislators to insist on the floor of behaviour below which they must not go.

There is a big and growing gap between the needs of children and the regulation in place, the digital world has transformed, but our protections for children have not kept apace. The U.S. is home to many of the companies that dominate the sector, what lawmakers in the U.S. do for children will ricochet around the world. How COPPA is reformed, the role and resource of the FTC and the willingness of this administration to put child protection top of its policy agenda, will impact on the lives of children everywhere.

In the UK, this is an issue that cuts across all party lines—it cuts across all ideological lines. I believe that the same strong consensus exists here, too. I have spent many years on this and wish to share whatever expertise I have. I stand ready to work with all of you. I hope that your committee will take up the challenge to lead the change. We are beyond the point of deciding whether this is a problem. It is time to work on the solution, and if I had to choose where to start—it would be with a comprehensive data protection bill which offers all children under 18 protections, by design and default.

I look forward to your questions.

Senator BLUMENTHAL. Thank you very, very much, Baroness. We will now begin 5-minute rounds of questioning. I will go to the Ranking Member after I finish and then, others on the Committee.

I think that the Baroness put it exactly right. These sites are extracting information, but also exploiting children. And parents cannot protect their children alone. Senator Graham and I introduced the EARN IT Act which, essentially, enables parents to fight the sexual grooming, exploitation, trafficking, torture, and rape of children. It is a real and present danger.

The statistic that one-quarter of all children are solicited on the Internet for illicit sexual purposes is just absolutely alarming and astonishing. And the EARN IT Act would create a narrow exception to Section 230 to empower survivors to stop the sharing of images and video of their sexual abuse. It is a narrow, exceedingly targeted exception to Section 230. And the question is for all the witnesses. Should we not broaden that kind of exemption, so that the sites themselves, not just the exploiters, are held accountable?

TikTok's failure to appear today, I think, is in some ways an admission that there are no adequate answers on its part to what is happening on that site. Sixty-six percent of all children use TikTok. And the idea that it is extracting this information, then exploiting it, but giving others an opportunity to do so, with the knowledge that it is happening, I think, argues powerfully for modifications in Section 230, perhaps incorporating the age-appropriate design code

that Baroness Kidron has championed so ably in the United Kingdom.

Let me begin with you, Professor Campbell. Should we modify Section 230?

Ms. CAMPBELL. I certainly think it is—I think it is something we need——

Senator BLUMENTHAL. I think you need your microphone.

Ms. CAMPBELL. We need to look at that question very carefully because I agree that many operators are getting away with conduct that, I will tell you, online would not be permitted. And therefore, because they do not—they are immune, or largely immune from prosecution, they have no incentive to stop. This same time, obviously, it needs to be narrowly tailored. It would need to pay attention to, not chilling speech that is protected by the First Amendment, and also harming small businesses who really cannot afford the kinds of litigation that might—but again, I do think that the idea is one that should be pursued.

Senator BLUMENTHAL. Thank you. Mr. Egelman.

Mr. EGELMAN. I think I would—I need to think about that a little bit more. The—I think there are things that could be done without touching on some of the free speech issues associated with Section 230, that would potentially, you know, do the same thing. Such as, you know, moving to the constructive knowledge standard and have other reporting requirements, you know, to strengthen COPPA without necessarily touching that. But honestly, I think I would need to think a little more about that.

I mean, my main concern is how that could—you know, unintended consequences of that. So, how that could be abused.

Senator BLUMENTHAL. Baroness Kidron.

Ms. KIDRON. Thank you. I think I am going to answer from the perspective of the Code, because one of the things that has really troubled me is that we have concentrated on what we do once we see somthing has happened—once—once children are being groomed. And I think that we have not considered enough, safety by design. And what we really need to start seeing now is proper platform accountability about its design features. For example, introducing strange adults to children as a normal piece of design, or making children very—very public. And at the same time, promoting a culture of popularity and of revealing, and so on. And I think there are a lot of things that we can do before we start on Section 230.

What I would say is that the failure to keep companies accountable for what they recommend, for what they rank, for what they promote, is quite different from accountability for what you host.

Senator BLUMENTHAL. Thank you. Would you agree, Professor Campbell—and I will ask the same question of the others—that Instagram should cancel its plans for Instagram Kids?

Ms. CAMPBELL. Yes.

Senator BLUMENTHAL. Mr. Egelman.

Mr. EGELMAN. Probably, yes. Yes, I will just leave it at that. I mean, I think concern there is just that—I guess I will not leave it at that. The concern there, I think, is even if the Instagram Kids is, you know, benign and is not collecting all of the data from kids, it is another type of grooming behavior, right? It is—it is locking

them in to the platform so that when they turn 13, all their friends are on Instagram. Now they are locked in and need to continue using it, and now it does start collecting all of their data. And then, they—you know, they are stuck making a choice. Do they abandon those social connection or, you know, give up privacy?

Senator BLUMENTHAL. Essentially, it grooms them, it prepares them, it extracts information, and it creates this web of involvement that is really perilous.

Mr. EGELMAN. Yes, exactly. And I think that one of the things that does come up a lot in the research, especially when looking at consumer perceptions about privacy, is this notion of learned helplessness. Where, you know, consumers just, you know, understand that they do not know how to, you know, tackle these privacy issues and have just, sort of, gotten accustomed to giving away their privacy because they do not really feel that they have a choice.

Senator BLUMENTHAL. Baroness Kidron.

Ms. KIDRON. I think, Chairman, you know, Facebook has not earned our trust to start doing children's services in this way. And I think, unless you have standards, unless you have agreement about what is a fitting platform for children, then of course, they should not go ahead and do this new platform. They cannot be trusted with children until we set out what that looks like.

Senator BLUMENTHAL. Facebook has not only failed to earn our trust, it has actually betrayed our trust, in many respects in its practices with Messenger Kids, allowing strangers to chat with children. Its other violations of trust certainly argue powerfully against, now, Instagram Kids. So, I hope that it will cancel its plans. Ranking Member Blackburn.

Senator BLACKBURN. Thank you, Mr. Chairman, and thank you to each of you for a very thoughtful discussion on this.

I have been hard at work at, what I call, the Virtual You Protection Agenda, which would be privacy, data security, some Section 230 reforms—tightening up the language there in Section 230—and then, dealing with antitrust. And I think it is time we realized these are not companies that are in their infancy. They are full grown companies. Their valuations are high. And they are very intentional in the moves that they make. And, Ms. Campbell, I appreciate your comments in regard to the intentionality of the moves that these companies are making, with how they data mine, and track, and utilize that information.

Baroness, I want to come to you first. You mentioned the contrast between the children's online age gaps in the U.S. compared to Europe. And in the U.S., where we do not consider an adult until you turn 18, but online children 13 and 14 can easily get full access to certain applications, without their parents permission. And I think this really leaves them vulnerable.

And we have mentioned Snapchat a couple of times and in 2019, I wrote a letter to the CEO of Snap, raising concerns about how child predators were arrested talking to underage children through this app. This is just—as a grandmother, I—that is something that you just have to say, how in the world can they not find a way to tighten up this process?

But you mentioned safety by design. So, how do you think that raising the online adulthood age would change the way that companies approach children's privacy on their apps? And talk to me a little bit about how companies in the UK and Europe have adapted to the changes that you all have made.

Ms. KIDRON. Yes, thank you for that question. And I think both the Chairman and you are speaking powerfully to the fact that the world of tech has transformed immeasurably, but the regulation has not kept up. And I do not think that the Internet founders had it in their mind that this was going to be the interlocutor of all childhood. And this habit, you know, taking the habits and thoughts and feelings of children and capturing them—you know, TikTok, Google, Facebook, Snap, and other unaccountable companies. And I think we should be worried that a child's latest selfie is stored for purposes yet to be decided in some server farm, whether that is in Hubei Province, in China, or in Nevada, USA.

So, I think that we have a global issue here, which is, as you say, you know, a child of 13 is not an adult and we must now extend our concern to children up until the age of 18. So, adults, we can discuss differently, but children, we have a duty of care to, and we must fulfill that duty of care.

To your point about the tech companies, I have a lot of conversations with engineers. And in fact, I always say, that if I had a pound, or indeed a dollar, for every time an engineer had said to me, "I have never thought about it like that before", I could actually finance our foundation from one end of the year to another.

What I mean by that is that we have to change our mindset. We have to think about what it means to be a child in that environment, and immediately, in relation to the code, what they had to do is actually disband direct messaging for certain age groups. They are not—they do not have the cognitive ability to work out whether that stranger is friend or foe. Just do not do it.

And in the code, it actually says, "Do not use their data to offer them detrimental material". And that is—you know, do not use their browsing history. Do not use the fact they hovered over something to then—to recommend it or rank it or put it into their feed. And so, I think that it is actually easier than we think.

What it is, is a commitment, is minimum standards, and it is a very, very clear enforcement path to say, this is what you must do. Not, this is what you could do or do a bit better, but this is what you must do. Because, actually, childhood is a precious stage and children do not grow up to be good adults unless they have decent childhoods.

Senator BLACKBURN. Thank you for that. Mr. Egelman, let me come to you. Talking about this privacy by design and you mentioned about how some of the companies are—use these personal identifiers and how these are used in concert with third-party data sets and algorithms, to build more accurate profiles of our children. Which is really a frightening thought when you look at the length of time that they can begin to gather that information and follow them.

So, talk to me a little bit about the safeguards that app developers could be using, in order to—to protect the children's PII.

Mr. EGELMAN. Yes, that is a really good question. It actually hits on a few points you brought up earlier, too. So, one of the biggest problems I see right now with COPPA, is that it shifts the compliance burden to lots of small developers who just really do not know what their obligations are. And then, invariably, you know, screw up by misconfiguring, you know, some third-party component that ends up sending data, you know, to advertisers or data aggregators.

There are also—certainly, there are also malicious actors, who are intentionally doing that in children's apps. But the net result is the same thing, right? At the end of the day, there is some third-party that is building dossiers of children. And whether the data was sent to them because, you know, the app developer knew they were doing that and, you know, because they get paid more to do it, or because something was just misconfigured, the app developers, essentially, have all the responsibility under the actual knowledge standard, right now. Because those third-parties, you know, just say, oh, well, we have no—we did not know that this is children's data and, therefore, we are not liable. And that is, currently, the state of the world.

I disagree, actually, with something that Professor Campbell said earlier, which is that it is difficult to figure out when apps are child directed. In many cases it is not. So, that information is public. Like, in the Google Play Store, when you download apps, there are categories. And if the app is in the kids' category, that means the developer actually went in there, when they uploaded the app, and clicked the button saying this is a child directed app. And to their credit, Google had a—you know, has a pop-up that asks them if they are in compliance with COPPA. And of course, they, you know, click yes and now, their app is suddenly available in the Play Store.

Anyone can actually just visit the Play Store or the Apple, you know, the iOS app store and see, you know, whether a given app is in the children's category or not, and then, use that information to realize that there is likely receiving data from children and take appropriate action, like delete it immediately and not do anything with it. But the fundamental problem is that they are receiving it.

A lot of the issues here come from this—the failure to adhere to privacy by design principles. And so, there is a whole framework, called Privacy by Design, that has several different principles. The most relevant here is data minimization. So, data should only be, you know, sent when absolutely necessary. In this case, you know, this hits on the internal operations exemption.

So, there are all of these exemptions for which these persistent identifiers can be collected and then, used for tracking purposes. But because there is ambiguity about what is considered internal operations, this data is being collected, even though it is not strictly needed.

So, an example of that, one of the carve outs is contextual advertising. So, contextual advertising is in contrast to behavioral advertising, where you are not receiving ads based on your, you know, history of what websites and apps, you have, you know, visited and played, but instead, you know, just what you are doing in the moment. So, what is the name of the current app? In theory, you

know, the marketing company, you know, is able to infer, given a user uses this app, you know, this is an appropriate ad to send them. So, maybe, like, an real estate app, you know, app is going to have ads for, you know, real estate agents, or something like that.

The point is, though, if it is all contextual, which is allowed under COPPA, by definition, they do not need the persistent identifiers to, you know, to figure out which individual user that is and create, you know, a dossier about them. And so, that is why, yes, I think data minimization, you know, would go a long way here.

Senator BLACKBURN. Thank you. I know my time is probably up.

Senator BLUMENTHAL. Thank you. We are going to go now to Senator Klobuchar.

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much. I want to thank you, Senator Blumenthal and Senator Blackburn for having this hearing. Such a timely, timely hearing. We all know that more kids have been online during the pandemic. But we also know that years of hearing, "trust me", from the social media platforms have not—has not worked.

So, I guess I will start with you, Ms. Campbell. In your testimony, you noted a complaint, filed with the FTC, that ultimately led to the 2019 YouTube settlement. And know you referenced (inaudible) opening. Do you think those (inaudible) or do you think we should be doing for holding these companies accountable?

Ms. CAMPBELL. I am sorry, Senator. I could not quite hear the last part of the—I heard you talking about YouTube——

Senator KLOBUCHAR. So, what more do you think—I am talking about what more should be done to hold the companies accountable with the YouTube settlement, yes.

Ms. CAMPBELL. Yes, OK.

Senator KLOBUCHAR. Mm-hmm.

Ms. CAMPBELL. Yes, and this actually relates to what Professor Egelman was talking about. Google, in the case of Google Play, does have a section called Designated for Families, and all of those ads—all of those apps that are available are supposed to comply with COPPA and they are supposed to not have any inappropriate advertising. They are not supposed to have a deceptive and unfair advertising techniques. There is just a number of, actually quite good, policies that Google has in place. The problem is that Google does not enforce them. And that is what his research showed and other—much other research has showed.

And that is why we also filled to a complaint against Google Play, asking the FTC to investigate whether it was making misrepresentations or—to the public about what it was doing. The FTC—this was filed in December 2018. The FTC did not take any action. We recently filed an update that cited some of this new research. And also, the fact that there was a major class action suit that was settled and will require at least some of these third-party companies—which are mostly companies people have never heard of, like, Applovin and Unity and Vungle and things like that—would require them to really clean up their business somewhat.

But I do think there is a lot more—it is not possible, even with all the resources in the world, for the FTC to go after every individual developer, and every different programmer that is uploading videos to YouTube. And so, therefore, I think the platforms need to be held accountable.

Senator KLOBUCHAR. Agreed. So, a report found—I guess this is for you, Mr. Egelman. A report found that more than 90 percent of U.S. parents believe that the Children's Online Privacy Protection Act, which only protects kids under 13, should be expanded to teens. Do you agree with expanding the protections?

Mr. EGELMAN. Absolutely. I mean, I think adults should have the same protections, you know, to opt out of this tracking when they, you know, so choose. But yes, no, I certainly think that the age should be increased.

Senator KLOBUCHAR. OK. We have been talking a lot about disinformation out there. Senator Luján and I led a letter to the CEOs of Facebook and Twitter, highlighting a report which found that approximately 65 percent of anti-vaccine content can be attributed to 12 individuals. We call then the Disinformation Dozen. Do you believe—and this can be for anyone on the panel—that the spread of misinformation online is particularly harmful for kids and teens? And not just about the vaccine, just misinformation in general. Baroness, if you want to take this, or anyone.

Ms. KIDRON. Yes, I would, and I think it is a really important point. And forgive me, but there is certainly a hailstorm in the background, if I sound a little funny.

You know, it is really quite crucial for children to trust and understand and grow to appreciate the nuance of information they are given. And they, themselves, repeatedly say that they are confused about what is true and what is false. And all the evidence points to the fact that they find it difficult to separate it out and it is destabilizing.

And I think that—that you are absolutely right to make the point that it is information, not only disinformation around health and so on, that we saw in the pandemic, but actually, they also report disinformation in terms of images about what they should look like, how they should behave. The truth that they are constantly presented with and they find it very, very problematic. And we have a duty to do better by them, as they grow up in a digital world.

Senator KLOBUCHAR. Very well said. Thank you. Thank you, everyone.

Senator BLUMENTHAL. Senator Markey.

STATEMENT OF HON. EDWARD MARKEY, U.S. SENATOR FROM MASSACHUSETTS

Senator MARKEY. Thank you, Mr. Chairman, very much. Thank you for having this very important hearing today. Thank you to Ranking Member Blackburn.

Protecting kids online has been a priority of mine for a long time and the COVID pandemic has actually made it even more clear. You know, the kids' use of this technology is just going through the roof and it is exposing even more problems that have existed for the last 20 years, in terms of kids' exposure to it. And it is why,

earlier this month, I introduced, with Senator Cassidy, a bipartisan Children's and Teens' Online Privacy Protection Act, which builds on the original COPPA law, the Child Online Privacy Protection Act, which I was the author of in 1998.

This new COPPA 2.0 helps to protect kids up to the age of 16—13, 14, 15-year-olds. The original law was just 12 and under. Not adequate, not in this new world that we live in. And it would require consent in order to collect information from them. It would also prohibit websites and apps from collecting more data than they need to fulfill the service that the teen is requesting.

The tech industry just loves getting all this information about children in our society. They just keep coming in on children, the tech industry, and gathering this information. The tech industry is just out of control on this issue. So, from my perspective, do you agree that young teens are an especially vulnerable audience that deserves much higher levels of protection?

Ms. CAMPBELL. Yes, I do.

Senator MARKEY. Do you agree with that, Mr.——

Mr. EGELMAN. Yes, absolutely.

Senator MARKEY.—Egelman. Yes, thank you. The legislation also includes a requirement that platforms should reasonably know that kids are on their websites and apps, to get parental consent, in order to collect children's data. After all, these companies have a lot of information about who is on their websites.

Ms. Campbell, can you quickly explain why this constructive knowledge standard will help protect children's privacy by stopping websites from turning a blind eye to the fact that kids are on their platforms?

Ms. CAMPBELL. Thank you, Senator. Under the current law, operator is not responsible for complying with COPPA unless their service or website is directed at children, or if they have, what is known as, actual knowledge. Which gives them the incentive to say, oh, we do not—we are not for kids. We do not have kids online. When in fact, they do know, because they are collecting so much information from these kids, that they can, you know, use this information to determine age. And often, you know, they also know because—TikTok, I do not know how they can say they do not when they—you know, there are so many articles about how kids are on the service.

So—so, yes, I do think that changing to constructive knowledge would make this an easier standard, both to apply and practice, but also for the companies themselves. I think the—it is a—it is a natural—it is like they knew, or they should have known. It does not really depend on whether they actually knew what the algorithm was doing. And I think, in Professor Egelman's testimony—written testimony, he also addresses——

Senator MARKEY. Yes, thank you.

Ms. CAMPBELL. Yes.

Senator MARKEY. And I know that you agree, as well, Mr. Egelman. So, let me—let me just say that I do think it is critical because of these tech firms and their exploitation of children. It is absolutely disgraceful what is going on. The tech industry just—you kick them in the heart, you are going to break your toe, in terms of their relationship with children in our society.

So, I just think we need to add a constructive knowledge standard. That is critical to protect children. And I believe that the Committee also should build on consent and disclosure requirements by enacting data use limitations. And one of those data use limitations should be outright ban on targeting advertising to children.

Ms. Kidron, do you agree that Congress should prohibit online advertisers from using children's data to target ads to them?

Ms. KIDRON. Yes, I do. Before I answer your question, Senator Markey, can I pay tribute to the work that you have done, for so many years, on behalf of children, and recognize that the world over, we know your name and the actions you have taken. So, I just want to make that clear from here in London.

Absolutely, targeted ads should be prohibited. Using children's data for that purpose is inappropriate. Contextual ads are perfectly adequate for the market. And I think that traditional communication law, both here in the UK and I believe in Congress, has already set out why it is unaccessible—unacceptable to bombard children with advertising.

You know, childhood is a journey. Children do not have the cognitive capacity and life experience to understand the high arts of advertising and influence.

Senator MARKEY. No, I appreciate that. Thank you so much. And Senator Blumenthal and I recently wrote a letter to Facebook CEO Mark Zuckerberg demanding answers about the social media company's plans for an Instagram plan to start bringing more children into their world. The company has yet to disclose all of the details of this plan, but it is clear that there are major risks to kids' privacy and well-being on this type of platform. Instagram for children sounds superficially very attractive, but we understand that it is a very vulnerable audience. Unfortunately, in its response to Senator Blumenthal and I, which I asked to be included in the record today——

Senator BLUMENTHAL. Without objection.

[The information referred to follows:]

Congress of the United States
Washington, DC 20515

April 5, 2021

Mark Zuckerberg
Chief Executive Officer
Facebook
1 Hacker Way
Menlo Park, CA 94025

Dear Mr. Zuckerberg:

We write regarding Facebook's recent announcement that it is "exploring" plans to launch a version of Instagram, which Facebook owns, for users under the age of 13.[1] Given Facebook's past failures to protect children and in light of evidence that using Instagram may pose a threat to young users' wellbeing, we have serious concerns about this proposal. Children are a uniquely vulnerable population online, and images of kids are highly sensitive data. Facebook has an obligation to ensure that any new platforms or projects targeting children put those users' welfare first, and we are skeptical that Facebook is prepared to fulfil this obligation.

Facebook has a record of failing to protect children's privacy and safety, casting serious doubt on its ability to do so on a version of Instagram that is marketed to children. In 2019, for example, reports showed that Facebook's Messenger Kids app, which was intended for kids between the ages of six and 12, contained a significant design flaw that allowed children to circumvent restrictions on online interactions. Specifically, Facebook allowed children using Messenger Kids to enter group chats with individuals who were not previously approved by the young users' parents.[2] Although software bugs are common, this episode illustrated the privacy threats to children online and evidenced Facebook's inability to protect the kids the company actively invited onto this platform. In light of these and other previous privacy and security issues on Facebook's platforms, we are not confident that Facebook will be able to adequately protect children's privacy on a version of Instagram for young users.

Moreover, research shows that apps such as Instagram may be detrimental to young people's wellbeing and mental health. A growing body of scholarship shows a link between young people's use of social media (and the devices they use to access social media) and the "increase in mental distress, self-injurious behavior and suicidality among youth."[3] New research shows

---

1 Ryan Mac & Craig Silverman, *Facebook Is Building An Instagram For Kids Under The Age Of 13*, Buzzfeed News (Mar. 18, 2021), https://www.buzzfeednews.com/article/ryanmac/facebook-instagram-for-children-under-13?mkt_tok=ODUwLVRBQS01MTEAAAF76Wa7gepI39A5wVlUsYMz6f2GDv9g1rWiYmtOlC3NziizWuTzJCaIshU83fHU8tAl9vVmx76IsbdGFY1iCyJpXpjzYB92I0S_GJGy5tDrIhYb.

[2] Russell Brandom, *Facebook design flaw let thousands of kids join chats with unauthorized users*, The Verge (Jul. 22, 2019), https://www.theverge.com/2019/7/22/20706250/facebook-messenger-kids-bug-chat-app-unauthorized-adults.

[3] Elia Abi-Jaoude et al., *Smartphones, Social Media Use and Youth Mental Health,* 192(6) CMAJ, 136–141 (2020).

that young people experiencing depressive symptoms are almost twice as likely to report using social media "almost constantly."[4] Although this statistic does not necessarily show a causal relationship, separate research shows that more than one in five young Instagram users are victims of bullying on the platform.[5] Parents and policymakers alike would generally benefit from additional research on the specific effects of social media use on children and teens, and certainly before your company encouraged children 12 and under to join. However, we already know today that there exists ample evidence to demonstrate the risks to kids' wellbeing that platforms such as Instagram can pose.

If Facebook's objective is to decrease the number of users under the age of 13 on its current Instagram platform, it should invest in efforts to do that directly. The alternative approach that Facebook appears poised to take—specifically, pushing kids to sign up for a new platform that may itself pose threats to young users' privacy and wellbeing—involves serious challenges and may do more harm than good.

In light of concerns outline above, we request responses to the following questions April 26, 2021:

1. Please describe in detail the model for a version of Instagram intended for children that Facebook is exploring.
    a. What specific user age range is Facebook considering for its version of Instagram for children?
    b. What data will Instagram collect about users on the version of the platform for children?
    c. Describe the relationship between the main Instagram platform and the children's platform.
        i. Will users on the children's platform be able to communicate with users on the main platform?
        ii. Will users on the main platform be able to view content posted on the children's platform?
        iii. Will accounts on the children's platform be affiliated with or created through accounts on the main platform? If so, will Instagram use data collected about a user on the children's platform to direct targeted advertisements at the affiliated user on the main platform?
    d. Describe how you will handle the data of a user on the version of Instagram for children when a user turns 13 years old.
    e. Describe how you will handle the data of a user on the version of Instagram for children when users delete or disable their accounts on the platform.
2. In what ways will the community guidelines and restrictions on certain types of content differ between the main Instagram platform and the version for children you are

[4] Victoria Rideout et al., *Coping with Covid-19*, Common Sense and Hopelab (2021), https://www.commonsensemedia.org/sites/default/files/uploads/research/2021-coping-with-covid19-full-report.pdf.
[5] *The Annual Bullying Survey 2017*, Ditch the Label (Jul. 2017), https://www.ditchthelabel.org/wp-content/uploads/2017/07/The-Annual-Bullying-Survey-2017-1.pdf.

planning?

3. Does Instagram use machine learning or other similar tools to identity users on the main Instagram platform that are likely children? If so, please describe what tools you use in this process, detail how that process works, and share how many child Instagram users you have identified through this process. If not, does Instagram have plans to use machine learning or other similar tools to identify child users on the main Instagram platform and move them to the version of the platform for children?

4. Will you commit that any platforms that Facebook launches for children, including a version of Instagram that is marketed for children, will never sell or share any user data with third parties for commercial purposes? If not, why not?

5. Will you commit that any platforms that Facebook launches for children, including a version of Instagram that is marketed for children, will always be completely free of targeted advertising? If not, why not?

6. Will you commit that any platforms that Facebook launches for children, including a version of Instagram that is marketed for children, will always be completely free of "influencer marketing" and other forms of commercial content that children may be incapable of identifying as advertisements? If not, why not?

7. Will you commit that any platforms that Facebook launches for children, including a version of Instagram that is marketed for children, will not employ "push alert" techniques or similar design features that encourage users to spend time on the app? If not, why not?

8. Will you commit that any platforms that Facebook launches for children, including a version of Instagram that is marketed for children, will not employ features such as "like" buttons, follower counts, or other tools that allow children to quantify popularity? If not, why not?

9. Will you commit that any platforms that Facebook launches for children, including a version of Instagram that is marketed for children, will not include beauty filters or similar design features that can lead to an unhealthy body image?

10. Will you commit that any platform that Facebook launches for children, including a version of Instagram that is marketed for children, will not include ephemeral features such as stories and "vanish mode" which are difficult to monitor for bullying or child exploitation?

11. Will you commit that a user of the version of Instagram for children will not automatically sign up a user up for the main version of Instagram when that user turns 13 years old? If not, why not?

12. Will you commit to turning on by default the most protective privacy settings, screen time limits, and any other parental control features available on the platform? If not, why not?

13. Will you commit to consistently subjecting any future version of Instagram for children to independent audits focused on privacy, marketing, and harmful content on the platform? If not, why not?

14. Please describe in detail the research you have conducted, commissioned, or consulted regarding the potential harms to children on social media platforms such as Instagram.

Should Facebook fail to provide adequate responses to the questions above or otherwise fail to demonstrate that a future version of Instagram for children would meet the highest standards of user protection, we would advise you to abandon your plans to launch this new platform.

Due to the telework policies of many congressional offices during the coronavirus pandemic, physical signatures are unavailable. The listed individuals have asked to be signatories to this letter. Thank you for your attention to this important matter. If you have any questions, please contact our offices.

Sincerely,

Edward J. Markey
United States Senator

Kathy Castor
Member of Congress

Lori Trahan
Member of Congress

Richard Blumenthal
United States Senator

Senator MARKEY. Facebook refused to give Senator Blumenthal and I any meaningful commitments about how to ensure that its proposed Instagram Kids app does not harm young users mental health and threaten their privacy. And that is why I am strongly urging Facebook to abandon its plans to launch a version of Instagram for kids. Ms. Campbell, do you share Senator Blumenthal and my concern about Facebook's proposal?

Ms. CAMPBELL. Yes, I do. I think it has already been discussed how they have not earned our trust. They have a bad track record. I was one of the signatories of a letter that asked them to stop it and I think, given the way—since Instagram—there are already lots of kids on Instagram. There are already—you know, it has some negative effects and to open it up to even younger children is, I just think, a huge mistake and a big risk.

Senator MARKEY. Yes. I think that, unfortunately, when it comes to putting children ahead of the profits, Big Tech always fails. They forfeited the benefit of the doubt on this issue. It is time for this Congress to pass comprehensive privacy legislation to protect children.

This goes on year after year after year after year. And we have to continue to wait and wait and wait and wait to put these protection on the books for our children in our country. They are being targeted. They are vulnerable. We know it is happening. We can pass a law this year to protect these children. We should put it at the top of our tech agenda.

Thank you, Mr. Chairman.

Senator BLUMENTHAL. Thank you, Senator Markey. And I strongly share your view that Facebook's response to us was abysmally inadequate on Instagram Kids, failing to address our reservations and concerns. And I think the impatience with Big Tech's invasion of privacy and exploitive practices is now very broadly felt and bipartisan, as is indicated by the comments that have been made today. And they should be on notice that, either they come to the table and participate in meaningful protection, or they will have failed to be part of this dialogue and there should be action this session. Thank you.

Senator MARKEY. Thank you, Mr. Chairman.

Senator BLUMENTHAL. Senator Lee.

STATEMENT OF HON. MIKE LEE,
U.S. SENATOR FROM UTAH

Senator LEE. Thank you, Mr. Chairman. Thanks to all of you for being here today. This is such an important topic and I share the passion that has been expressed by my colleagues on both sides of the aisle here. These are things that we need to address.

In the past there have been a handful of factors that have, at times, slowed progress or, in some cases, even reversed it. Some of them are technical; others are constitutional. Sometimes the technical and the constitutional merge.

As—as you are aware, in order to survive a First Amendment challenge, where the First Amendment is implicated, if you have got a government action that interferes with free speech, you have got to be able to survive strict scrutiny. Which means that you have got to show that the government action, at issue, is directed

at something, as to which, there is a compelling state interest. A compelling governmental interest must be the object of the legislation. And it must further that compelling state interest in the least intrusive, least restrictive means—through the least restrictive means possible.

At times, this has become a problem, as—as we learned in 1997 in a case called *Reno v. ACLU*. In that case, the Supreme Court of the United States invalidated provisions of the Communications Decency Act. Provisions that would have prohibited the transmission of certain indecent content to minors.

Now, in that case, as I recall, the Supreme Court concluded that the online harm and the risk of online harm to children, was itself a compelling governmental interest. But the provisions at issue did not provide the least restrictive means to achieve that compelling state interest. Specifically, the court found that the age verification process for children, at the time, simply was not viable and would potentially prohibit access of others who should not be prohibited from accessing such content.

Now, that was back in 1997. 1997, I think, was the year I purchased my first cell phone, and it was a relatively decent phone, at the time. It just made phone calls. It did not do anything else, nothing else at all. And we were, of course, a decade away from anything resembling an iPhone. But since then, things have changed.

So, Professor Campbell, in your view, has technology advance sufficiently since 1997, such that age verification is now a reality, in a way that it might not have been then? Could we overcome this hurdle now?

Ms. CAMPBELL. I cannot really speak so much to technology. I do know that, as part of this data collection, that companies often will infer, or these advertising networks will be able to infer the age of the users, so that it may well be much—I mean, certainly it would be more possible today than it was in 1997. And also, I mean, there are just so many more kids online and everyone online doing—using it for so many different purposes. And in just so many ways, the world is completely different than it was in 1997.

Senator LEE. From that, one could certainly argue that our ability today to use the least restrictive means of furthering a compelling state interest is significantly enhanced, relative to what it was 24 years ago.

Ms. CAMPBELL. Yes. I think so. But I also want to point out that commercial speech, at least this deceptive, is not permitted to children. That—we—with children are different than adults, in that, we as adults have some responsibility for their—their well-being. And so, there are certain things that we would not permit to be regulated as to adults, we do permit to be regulated as to children.

Senator LEE. Sure.

Ms. CAMPBELL. And so——

Senator LEE. So, once you enter into the territory of Central Hudson, then if it is—if it is deceptive, you may have other tools that will not, themselves, trigger strict scrutiny.

Ms. CAMPBELL. That is correct.

Senator LEE. Now, online platforms gather a lot of data with regard to their users. Understandably so. I mean, this is their busi-

ness. They want to understand. They want to make sense of the marketplace in order to facilitate targeted advertising. That is how many, if not most, of them make a living. But I am concerned about what that can mean, at times, with respect to children and how they target children. And what they are doing, or not doing, to protect children.

Baroness Kidron, do—do online companies know, or if they do not know, should they know—should they be expected and required to know the age of the minors who have profiles on their respective platforms?

Ms. KIDRON. Yes, Senator. I think—if I could just point at something that happened a couple of weeks ago in Australia, where researchers asked to find 13- to 17-year-olds with an interest in alcohol, smoking, gambling, extreme weight loss, fast foods, online dating services. Those were 13- to 17-year-olds. And they were then able to fabricate ads mentioning prizes, cocktails, and asking them if they were Summer ready.

You see how insidious it is. So, it is not even just should they know, could they know, to which it is an unequivocal yes, it is even when they do know, they are not treating them properly. And if I might also just say, narrowly to your point that you just asked previously, is 5Rights recently wrote a report about age assurance, "How Do They Know How Old We Are?" And I have sent it to the Committee, and I think what is absolutely true in your observation is very sophisticated.

It is, indeed, the case that things have changed. We do have technology. What we do not have is governance, transparency, and an agreement about what age assurance should be, how it should be properly deployed.

So, I think the answer to both your question is, you know, we do have the means. We do not yet have the will.

Senator LEE. Mr. Chairman, I realize my time has expired. Could I ask one follow-up question——

Senator BLUMENTHAL. Sure.

Senator LEE. That leads naturally? Thank you very much. Baroness, I would like to go back to you for a moment and follow up on an observation you just made. I have learned a lot about this from a number of experts in the field, and especially, my friend Melissa McKay from Utah, who has done a lot of work educating parents and children about the risks associated with content that can be obtained online, very often through social media platforms, by children.

Sometimes the content is delivered to them, with full knowledge of how old they are, because of the fact that, when they open an account, they are required to provide certain information about their age. And even with that, sometimes one could argue because of that, they receive awful, awful content delivered to them, knowing what they have.

And yet, these apps—these social media platforms often operate through apps that are, themselves, subject to app age appropriateness ratings on the Google app store, and also on the Apple app store. And in many instances, these age appropriateness app ratings on the app stores indicate that the apps themselves are suit-

able for children, in other cases for teenagers, including young teenagers.

So, why—why is there such a disparity sometimes, between the apps listed age appropriateness rating and the content available on that platform, and sometimes sent to a minor—to a child, on that platform? Why the disparity?

Ms. KIDRON. Yes, I mean, well, I think you maybe needed to ask TikTok, if only they would show. No, I think the truth is, in fact, I should revise that and say, Google and Apple. I have raised this question in Parliament. I have raised it more than once. And I think it is extraordinary that we do not have a regulation or a law that says the app store must give the same age rating as the terms and conditions. But in fact, we go on, consistently, and find many, many apps that are labeled one thing—nine, 10, you know, very young ages that then turn out to be 16 and 18. And it is something I will be turning my attention to and I hope it is something the Committee will turn its attention to.

I think the other thing that I would like to say to you is that, recently, we did some research—again, we will be publishing it shortly. But it was the case that we were able—we could see a child being targeted with, actually, government safety information. But that same child was being targeted with self-harm material. In one case, a very, very aggressive adult pornography, and so on.

And I think this point, that I am trying to make is, yes, we can find out they are children. And there are new ways of looking at age assurance that are data-light and do not interfere with other users. But also, we have to extend and put in protections for those users that they know are children. I mean, this is just essential.

Senator LEE. Thank you, Baroness. Really appreciate that and I would love to work with you in that effort. Thank you, Mr. Chairman.

Senator BLUMENTHAL. Thanks, Senator Lee. Senator Luján.

STATEMENT OF HON. BEN RAY LUJÁN,
U.S. SENATOR FROM NEW MEXICO

Senator LUJÁN. Thank you, Chairman Blumenthal, and thank you to you and to Ranking Member Blackburn for addressing this urgent subject.

Child safety online is a pressing issue in New Mexico. My home state is currently pursuing multiple court cases to hold companies accountable when they violate child privacy laws. I am grateful for New Mexico's leadership in protecting the safety and privacy of young children online.

Ms. Campbell, in one of these cases, Google is accused of improperly collecting students physical location, browsing history, search history, contacts, and even voice recordings, through its educational products. Google is used in over half of American public schools for its free products, and I do not believe that parents should have to choose between their child's privacy and their education.

Ms. Campbell, yes or no, do believe collecting data for advertising purposes is ever appropriate in the classroom?

Ms. CAMPBELL. No, it is not.

Senator LUJÁN. Dr. Egelman, I know you have worked closely on one of those New Mexico cases. In fact, your lab was among the

first to publicly report violations by Tiny Lab Productions to Google. In that case, Google first reviewed the app under question when it was submitted to its Designed for Families. That is a program that they have. And again, after you alerted the company, still Google did not immediately classify the game as being primarily directed to children, despite clear advertising that the game was for kids and would "keep them entertained for hours". And those are all quotes—"keep them entertained for hours", "right from Google", "for kids", "primarily directed to children".

Google eventually changed course, but it took months for it to terminate the developer. By that time, the app had already been downloaded millions of times. Yes or no, to ensure that these apps do not take advantage of children, should Google reform its app review process?

Mr. EGELMAN. Absolutely, yes.

Senator LUJÁN. What recommendations do you have there, Mr. Egelman, for reform?

Mr. EGELMAN. I think one of the biggest problems is that there is not really a review process. So, Google has policies that they post that, you know, developers are supposed to abide by, including, you know, checklists that developers check to say, my app is in compliance with COPPA. And that is pretty much the end of it. And so, I think that, you know, there should be some proactive auditing of apps.

And actually, to their credit, it looks like Google is starting to shift in that way. I do not know if you saw their announcement, guess it was a week or two ago, where they are now following Apple's lead with the privacy nutrition labels. And if I remember correctly, I think one of the things that they mentioned in that statement about that program that they were going to be starting, was just that they might, you know, start including certifications from third-parties that have done privacy audits on apps. And so, I think that would, absolutely, be a step in the right direction.

I mean, I think that—honestly, I think that this is an opportunity to actually have—you know, to create some robust competition around this by having, you know, private entities that have rigorous standards that are, you know, public and maybe regulated by the FTC. Because frankly, I think, if Google did say that, you know, they are changing their internal review processes, most people probably just would not believe them. And it would be hard to tell, as an outsider, what exactly they are doing. And so, I think that is why, you know, outside forces are necessary here.

Senator LUJÁN. Appreciate that. Ms. Campbell, in your 2019 testimony to Congress, you reported that the FTC had no formal process for parents to file complaints or obtain relief for COPPA violations. What is more, of the 14 requests you filed to the FTC to investigate COPPA violations, none have been responded to.

Two questions—has any of that changed? And what can parents do when they suspect a child's data is being illegally collected?

Ms. CAMPBELL. Well, there is still no formal process of complaints. There is maybe some indication that the FTC is looking at these questions a little more. They did issue these 6B investigative demands, so that they could understand better what is going on in

the marketplace and what is happening to children. So, I think that is a positive step.

But I think parents should complain. Just because there is no complaint form you need to fill out, does not mean you should not complain. You should definitely let them know what is happening and what your concerns are. And they can also get in touch with groups like Campaign for a Commercial Free Childhood and other groups that are working to try to get the government to be more responsive to protecting children.

Senator LUJÁN. Thank you. And, Mr. Chairman, I do have some other questions, but I will submit them into the record for response, as well. And I just want to thank all the witnesses for their time today and the work that they are doing and their commitment to protecting children, as well.

With that, Mr. Chairman, I yield back. Thank you.

Senator BLUMENTHAL. Thank you, Senator Luján. I have just a few more questions and then, if the Ranking Member has some I will call on her.

Dr. Egelman, last August, AppCensus, a research firm that you have helped to lead, discovered that women's health app, Premom, was sharing deeply sensitive health information with Chinese advertisers. Senator Klobuchar and I and a few other colleagues, sent a letter to the FTC urging it to investigate Premom. We are concerned that it is a privacy threat and a national security risk.

These app stores are essentially the Wild West. Consumers have no way of knowing whether an app is child-safe or secretly selling data to Chinese data brokers. I would also mention my continued concerns about TikTok's deep links with China, as well as the FTC's deception case in 2020, against a subsidiary of the Chinese firm, Tencent. I suspect that a lot of these children's apps and digitally connected toys have substantial issues with sharing data to Chinese firms.

From your research, how extensive is the problem of children's app developers sharing kids' personal data with Chinese firms?

Mr. EGELMAN. That was actually how we started this line of research. That is a prescient question. When we—I mean, this whole thing with the children's apps specifically—you know, as I said I have been—my lab has been building instrumentation so that we can monitor mobile apps to see what they do. And in the course of that, we started, you know, playing with some kids' apps because there is law in that area that should be governing them.

But one of the first ones we found was an app, I think, targeted at, like, five and under in the Google Play Store that, yes, had several, you know, trackers going to Chinese companies. And then, that is when we started digging deeper and found that this is relatively pervasive.

The Premom finding that you mentioned, was actually pretty insidious because the way that they are transferring the data is likely to not be detected by most people examining the app. And so, you know, it is—it is hard to tell, in this particular case, and probably many other cases where, you know, apps are going—you know, apps are sending data to many of these third-parties because, again, in some—you know, given—given how obfuscated

these transmissions were, it is possible that app developers just have no idea that their apps are doing this.

And I think that is part of the problem here is that the app developers—you know, I started to elude to this earlier, but I guess I did not finish that thought, which is just that, the compliance burden is put on the individual app developers. And there are, you know, millions of them, right? There are millions of apps.

But most of the concerning uses of the data here are, you know, going to data aggregators and advertising companies and there are comparatively fewer of those. And they are the ones who actually, you know, control the data and, you know, have the ability to use it for, you know, these harmful things.

And so, you know, that is one advantage of switching to the constructive knowledge standard, which is, that shifts the compliance burden to those third-parties, substantially. And they are in the best position to actually do the enforcement here to, you know, shut off, you know, those data flows. And if they do not then, you know, action should be taken against them. Because they know what apps are sending them the data, even if the app developers do not know that the data is being sent to them.

Senator BLUMENTHAL. Well, who would those third-parties be?

Mr. EGELMAN. You know, the makers of third-party components like, you know, Facebook has components in—I might need to correct this exact number, but it is on the order of, like, 30 to 40 percent of the apps that we have looked at have Facebook code in them, which gives them the ability to send data to Facebook. And you know, Facebook's SDK, software development kit, is the, you know, premade components that developers download and stick in their apps. It is——

Senator BLUMENTHAL. You would shift the burden?

Mr. EGELMAN. Yes, it would shift the burden to organizations like Facebook.

Senator BLUMENTHAL. They have not only the visibility——

Mr. EGELMAN. Yep.

Senator BLUMENTHAL.—but also, the resources.

Mr. EGELMAN. Exactly.

Senator BLUMENTHAL. And they have the resources to compensate women whose data is shared, without their knowledge and consent, violating their privacy, potentially leading to exploitation of them, for harms that are done, correct?

Mr. EGELMAN. Yes.

Senator BLUMENTHAL. So, they should be held accountable—Facebook.

Mr. EGELMAN. Absolutely. And all of the other—I mean, Facebook it is—you know, Facebook is big and, you know, they have user facing services. But there are also, you know, lots of these companies that most consumers have never heard of before, that are also collecting, you know, large amounts of data from children and adults, often without, you know, the consumer's knowledge. And also, often without the app developer's knowledge because they might have misconfigured something, or it is just really obfuscated and intentionally trying to deceive the app developer.

Senator BLUMENTHAL. And we cannot depend on the FTC to do it alone.

Mr. EGELMAN. No, I mean, like, this is—the big problem is, you know, again, the FTC does a lot of really good work and they have knowledgeable people. But they bring less than two cases a year, because they just do not have the resources. I mean, unless we are going to entertain——

Senator BLUMENTHAL. Even if we give them the resources.

Mr. EGELMAN. Right, well, I mean, even if you entertain giving them, like, a DOD style, you know, size budget, like, I still do not think the problem is going to be fully, you know, under control. I think that, you know, there are a lot of different facets here and, you know, these are complicated problems.

Senator BLUMENTHAL. So, we ought to give the FTC more resources?

Mr. EGELMAN. Yes, absolutely.

Senator BLUMENTHAL. That is a thumbs up.

Mr. EGELMAN. Yes, absolutely.

Senator BLUMENTHAL. But even with those additional resources, we need other means of holding Facebook and the tech platforms accountable?

Mr. EGELMAN. Yes—yes, because right now, without the resources to, you know, bring cases, it is essentially an unfunded mandate.

Senator BLUMENTHAL. Exactly. Let me ask you, Professor Campbell, about influencer guidelines. I know you have done a lot of work on this issue. The FTC released guidelines for online influencers. You know how pervasive their impact can be on kids. But these guidelines failed to sufficiently address the advertising that is targeted to children, nor are they fully enforced. Numerous unboxing videos on YouTube are, in actuality, people paid to promote toys, games, and other products to unsuspecting children.

I am encouraged by the FTC's request for comments on its endorsement guidelines, but I think a lot more has to be done. And I have repeatedly raised my concerns to the FTC that these influencers are manipulating and targeting children, and often pushing dangerous products. Tell me what you think need to be made in the FTC's influencer guidelines?

Ms. CAMPBELL. Yes, I agree with you. In my testimony, I talk about how, on YouTube, three of the top five channels viewed in the U.S. are targeted at children and they feature child influencers. And so, these kids make lots of money. Not all kids make lots of money, but these—you know, the top ones really make a lot of money and sometimes they are promoting, you know, sugary cereals or candy. And other times, they are promoting toys—that is what a lot of the unboxing videos are about—or even promoting their own lines of products, as in the case with, I think her name is, Diana. And I included a picture in the—in my testimony where she—it is a 10-minute video and then, she—she becomes a doll, herself, that you can then buy online.

So, it is a big problem. And the FTC—the problem is—one is largely enforcement. I mean, this is a huge business, and the FTC just is not enforcing its guidelines, as it is. But the other thing is, when they do—and they have not brought any cases involving children—programming directed at children. When they do bring cases, they—they merely require that the sponsorship be disclosed.

And that is problematic for kids because—well, first on, you can hardly see the sponsorship identifications, if they are even there. Especially when you are looking at, like, TikTok where there are, like, 25 different hashtags and one will say #ad.

But they also just do not really understand that the purpose of these videos is to sell products. I mean, for little children, they think that EvanTube and Ryan and Diana are their friends. And they—you know, they do not—they have the—they enter into what is called a parasocial relationship with these actual children—child celebrities as well as spokes characters—you know, cartoon celebrities that are popular with children. And so, they really cannot—they just do not have the cognitive capacity to fend against that, even if they are told it is advertising. Of course, a lot of them cannot read, either.

So, I think the Commission needs to clearly recognize that, and say for kids that do not have this capacity, you just cannot have this kind of programming. It is not enough just to disclose it.

Senator BLUMENTHAL. Thank you. You know, I think that parents often are unaware of the impacts of this kind of manipulative advertising on children. Last week, the Center for Digital Democracy released a report describing how Big Tech is helping to fuel the childhood obesity crisis. Junk food, e-cigarettes, vaping—they have all been pushed to children, targeted to them. Tech platforms are harvesting troves of information that enable targeting of children by companies that produce these products.

It is not just junk food. In fact, the e-cigarette company, Juul, bought ads across sites like "Cartoon Network" and "Seventeen" magazine to target young audiences. This innovative and absolutely reckless tracking and targeting of children is a real public health menace.

How is it that data collected from kids' apps is fueling these sophisticated ad campaigns and profiling to push these harmful products?

Ms. CAMPBELL. Well, I think one of the biggest problems is that the whole process of collection and how the data is used is not transparent, at all, and it is very complicated. And most people do not understand it, myself including. I would say I do not fully understand it. But I do know that, if you do not know it is happening—and then, as a parent, you know, if your child is using their tablet, or their computer, for schoolwork or a phone, they are not seeing what the child is seeing. And yet, there is—so, they do not know about it and of course, they have not been asked.

When we were looking into apps on the Google Play Store, that were in the Designed for Families program, we found that a lot of them had advertising for things like gambling, for alcohol, and also, just things that really were not appropriate for children. So, I—did I answer your question?

Senator BLUMENTHAL. You did. Both of you have filed substantive complaints to the FTC about violations of COPPA. As you observed, I think, Mr. Egelman, in the last 21 years, only 34 COPPA cases have been filed by the FTC. That is plainly a lack of enforcement that may be due to lack of resources. But it also may be due to lack of will or vigor, in some administration. And my hope is that we will see an end to, what you have called, ramp-

ant non-compliance. I would call it the Wild West. And like the Wild West, it is increasingly perilous to kids and my hope is that the FTC will be a stronger and more vigorous partner in enforcement going forward.

I want to thank all of the panel. Thank you, Baroness. Thank you to both of you present here today. This has been a very valuable session and on behalf of my colleagues, we express our gratitude to you and keep up the good work. Thank you.

This record will remain open for a week. A number of colleagues have indicated they want to submit additional questions and for now, it is closed. Thank you.

[Whereupon, at 11:46 a.m., the Committee was adjourned.]

APPENDIX

May 13, 2021

Hon. Richard Blumenthal
Chairman
Subcommittee on Consumer Protection, Product Safety, and Data Security
U.S. Senate
Hart Senate Office Building 420 A
Washington DC, 20510

Hon. Marsha Blackburn
Ranking Member
Subcommittee on Consumer Protection, Product Safety, and Data Security
U.S. Senate
Hart Senate Office Building 420 A
Washington DC, 20510

Dear Chairman Blumenthal and Ranking Member Blackburn:

On behalf of Common Sense, a national nonprofit organization dedicated to helping kids and families thrive in a world of media and technology, we respectfully submit our recent paper entitled *AdTech and Kids: Behavioral Ads Need a Timeou*t for inclusion in the record of the May 18th hearing, "Protecting Kids Online: Internet Privacy and Manipulative Marketing," held by the the U.S. Senate Subcommittee on Consumer Protection, Product Safety, and Data Security.

This paper examines the practice of behaviorally targeted advertising, the harms it poses for young people, and what policymakers and companies can do to improve the landscape. More "relevant", personalized, and microtargeted ads are not desired by or beneficial to kids and families. This model encourages tech companies, large and small, to profile kids and manipulate their emotions for commercial ends. We thank the subcommittee for their attention to this critical issue and hope this paper can be helpful as members examine how to best protect children and teens' privacy online. Please feel free to reach out if I can be of further assistance.

Sincerely,

Ariel Fox Johnson
Senior Counsel, Global Policy
Common Sense

Cc: Members of the Subcommittee on Consumer Protection, Product Safety, and Data Security

www.commonsense.org 699 8th Street, Suite C150, San Francisco, CA 94103 • (415) 863-0600


AdTech and Kids:
Behavioral Ads
Need a Time-Out
common sense

AdTech and Kids:
Behavioral Ads Need a Time-Out

By Joseph Jerome and Ariel Fox Johnson

Summary

The many "free" online services that kids and families rely on come at the high price of privacy. For years, apps and services have been subsidized by their users' information, feeding an ad-supported model that tracks and profiles kids, manipulating them and microtargeting them and their families with ads and content that companies think are relevant. Big tech companies have convinced advertisers and marketers that the more targeted ads are, the better,[1] but this business model has underappreciated costs, especially for kids. It's underlying profitability also is questionable. In this paper, we examine the practice of behaviorally targeted advertising, the harms it poses for young people, and what policymakers and companies can do to improve the landscape.

Behaviorally targeted ads are now standard fare for online platforms, and they are big business. But the truth is, behaviorally targeted ads are bad for kids. First, kids do not want or understand targeted ads. The majority of kids and parents feel uncomfortable with their data being used for targeted advertising.[2] Children and teens cannot comprehend the full complexity of how their personal information is collected, analyzed, and used for commercial purposes.[3] Second, young people are particularly vulnerable to manipulative marketing practices, and personally targeted advertisements exacerbate this problem. Third, we should question the utility of tracking, profiling, and commercially manipulating young people during their formative years, when their brains are malleable and we should be encouraging exploration and trying new things. Whatever questionable benefits may accrue for advertisers is not worth the damage behavioral ads cause to our privacy, our society, and even our democracy. Common Sense believes that children and teens should neither be tracked and profiled online nor subject to behavioral ads based on their personal information or online activity.[4]

Understanding behaviorally targeted ads

Online advertising has been called the "original sin" of the internet.[5] From the birth of the first digital banner ad in 1994, online advertising has been the dominant business model for websites, mobile apps, and digital services. Problems emerged from the start. While early internet users were barraged by obnoxious pop-up ads, advertisers became obsessed with trying to understand how their online ads performed—who was seeing them and how users responded.[6] Small text files known as cookies became the answer. These files, which initially were created as a way for websites to remember information about the same visitor over time, became a way to track and surveil online behavior at an unprecedented scale.

Over the past three decades, online advertising has become a complicated and confusing ecosystem. Initially, online advertising operated similarly to ads placed in magazines and newspapers: Relying on readership demographics or the contents of a paper, an advertiser would pay to place an advertisement for, for example, cruises in a travel section that every subscriber would see. Online, that cruise ad would be placed on a travel blog, cookware ads on a recipe site, or exercise equipment on a health app.

---

[1] Mahdawi, A. (Nov. 5, 2019). Targeted ads are one of the world's most destructive trends. Here's why. *The Guardian*.

[2] Information Commissioner's Office. (2019). Towards a better digital future informing the Age Appropriate Design Code, revealing reality.

[3] Gelman, S. A., Martinez, M., Davidson, N. S., & Noles, N. S. Developing digital privacy: Children's moral judgments concerning mobile GPS devices. *Child Development 2018, 89*(1), 17–26.

[4] Common Sense Media. (2018). Privacy matters: Protecting digital privacy for parents and kids.

[5] Zuckerman, E. (Aug. 14, 2014). The internet's original sin. *The Atlantic*.

[6] Polonetsky, J., & Gray, S. (Nov. 2015). Cross device: Understanding the state of state management. Future of Privacy Forum.

Advertisers became convinced that ever more targeted advertising, personalized to each user, would be more profitable. Today, online advertising has shifted away from the contextual model above to a more personalized model that collects huge quantities of data about an individual's location, their device, internet searches, and even which social media posts a person is hovering their mouse over. Also collecting information are data brokers, who add data to profiles and data segments of third-party ads.[7] This information collectathon is used to guess our hobbies and interests and infer religion, wealth, and marital status.

Thousands of companies are involved in what is known as adtech, or providing advertising technologies.[8] This creates a complicated soup of acronyms: SSPs, DSPs, DMPs, and on and on.[9] Data brokers and location aggregators also have gotten into this mix. Seemingly innocuous banner ads on websites are actually visible manifestations of a complex system that tracks individuals across websites and apps, devices, and the real world. Now, advertisers use data collected over time and from different places, online and off, to understand our behaviors and guess at what we may like next.[10] These insights are then used to target us with ads that businesses think are relevant—teens and, often, younger children are caught up in this process. Often this targeting is completely automated and happens in milliseconds through a real-time bidding process that occurs as websites load.[11]

Defining adtech

What is contextual advertising?
Contextual advertising relies on ads displaying based on a website's content. Think: placing an ad for dishware on a recipe site, or an ad for running shoes on a running forum. There are more sophisticated types of contextual targeting that rely on categorizing or assigning keywords to specific online content.[12]

What is behavioral advertising?
Behavioral advertising relies on web browsing behavior such as pages visited, searches performed, and links clicked to categorize and profile internet users. Mobile and brick-and-mortar information also can be added to this mix, creating a more detailed profile.

What is programmatic advertising?
Programmatic ad buying refers to the use of software to purchase digital advertising rather than relying on individual deals or human negotiations. Much of online advertising is done this way.

What is real-time bidding?
Real-time bidding involves the buying and selling of online ad impressions through real-time auctions run by ad exchanges that occur in the time it takes a webpage to load.

[7] Jerome, J. (Sept. 25, 2018). Where are the data brokers?. Slate.
[8] Brinker, S. (2017). Marketing technology landscape supergraphic (2017): Martech 5000. Retrieved from http://chiefmartech.com.
[9] Digiday. (2015). Programmatic advertising in 6 easy steps.
[10] Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. *PublicAffairs*, p. 96.
[11] Marshall, J. (Feb. 20, 2014). WTF is programmatic advertising?. Digiday; Marshall, J. (Feb. 17, 2014). WTF is real-time bidding?. Digiday.
[12] Criteo. (Nov. 1, 2018). Targeting 101: Contextual vs. behavioral targeting.

Behaviorally targeted ads harm kids

While advertisers insist on the value of targeted ads, pediatricians and child health experts continue to marshal evidence of the particular harms that targeted ads present for children.[13] Kids get swept into this ecosystem due to gaps in the Children's Online Privacy Protect Act, a lack of protections for teens between the ages of 13 and 18, and ads targeting households that include children.

First, kids don't want behavioral ads. While advertisers promote the perceived benefits of "tailored advertising,"[14] young people are not interested in the value proposition of behavioral ad targeting. They express negative attitudes about data collection and sharing, especially surreptitious collection, disliking when apps monitor or collect "private information about them."[15] When they have actually been consulted about this, children express irritation that a game they are playing might watch them ("if they watched me when I was playing, then I don't like that"), and teens say companies should "[s]top selling our data, phone numbers, etc. to companies, for advertisements."[16] In a survey by the Irish Data Protection Commission, kids called targeted ads "annoying," "unfair," and "an invasion of privacy."[17]

Kids do grasp that behavioral ads are different in degree than traditional advertising. As the Irish Data Protection Commission explained, kids recalled "unsettling experiences of being 'followed' by personalized ads on the internet, and one group of eight to nine year olds drew parallels between TV ads and online ads, saying that online ads 'are so scary because they are pointed at you directly and not at everyone like a TV ad.'" One respondent even said, "It feels like they're stalking you."[18] These concerns echo research from Common Sense, which has found that over two-thirds of teens are worried that social networking sites use their data to allow advertisers to target them with ads.[19]

> *Researchers have concluded that children are not equipped to identify targeted ads that exploit their tracked activity data.*

Second, kids are largely defenseless against advanced and personalized targeting techniques that they do not understand. Advertising and marketing in general have a powerful effect on children. Studies demonstrate that ads quickly affect kids' desires and purchase requests, and parent-child conflicts can occur whenever parents or caretakers deny those requests precipitated by advertising.[20] Pediatricians recognize that children are

---

[13] Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2019). *Privacy risks and harms*. Retrieved from Common Sense website: https://privacy.commonsense.org/resource/privacy-risks-harms-report

[14] Network Advertising Initiative. (2020). Understanding online advertising: How does it benefit me?

[15] Anonymous. (May 8–13, 2021). "They see you're a girl if you pick a pink robot with a skirt": How children conceptualize data processing and digital privacy risks. *CHI '21: ACM CHI Conference on Human Factors in Computing Systems.*

[16] Anonymous. (May 8–13, 2021). "They see you're a girl if you pick a pink robot with a skirt": How children conceptualize data processing and digital privacy risks. *CHI '21: ACM CHI Conference on Human Factors in Computing Systems*; 5Rights Foundation. (March 2021). But how do they know it is a child? Age assurance in the digital world.

[17] Data Protection Commission. (Jan. 28, 2019). Know your rights and have your say! A consultation by the Data Protection Commission on the processing of children's personal data and the rights of children as data subjects under the General Data Protection Regulation.

[18] Data Protection Commission. (2019). Some stuff you just want to keep private.

[19] Common Sense Media. (2018). Privacy matters: Protecting digital privacy for parents and kids.

[20] Robertson, T. (1979). Parental mediation of advertising effects. *Journal of Communication, 29(1)*, 12–25.

particularly vulnerable to commercial manipulation. Young children cannot distinguish commercial and noncommercial content, while most children younger than 8 years of age cannot identify ads or recognize the persuasive intent of commercial appeals.[21] Many older children up to age 12 have trouble identifying and/or understanding the commercial intent of an advertisement.[22] Even advertising professionals acknowledge that children are a vulnerable advertising target group.[23]

Behavioral advertising and the data collecting and profiling that support it exacerbate this problematic situation. Marketers and data brokers can create dossiers of a young person's interests, fine-tuning sales pitches to impressionable audiences who, as discussed above, may not even understand that they are seeing ads, especially in complex digital environments.[24] Most children do not realize that ads can be customized to them.[25] Kids do not grasp the scale of how ad networks work, and that different ads show up for different kids even in the same game. Researchers have concluded that children are not equipped to identify targeted ads that exploit their tracked activity data.[26]

> *Targeted ads can expose aspects of teens' lives they would prefer to share on their own terms, and the consequences of being inadvertently outed and exposed can be worse for kids without legal autonomy.*

Finally, behavioral profiling is particularly problematic for kids. This ad targeting and associated data collection and profiling occur at a unique time of development in kids' lives. Children's brains and identities are developing and forming. It is a time when society encourages children to explore new things and not worry about making mistakes. The constant profiling that accompanies behavioral ad targeting, and targeted ads themselves, do a disservice to kids by potentially labeling and limiting them. Kids' choices and their autonomy may be constrained and shaped by coercive techniques that only show them certain opportunities but not others—as with, for example, women being shown fewer prestigious job offers in search results[27]—and by algorithmic profiling that builds in bias when determining whether to, say, admit students into educational programs.[28] And kids can hold

---

[21] Wilcox, B. L., et al. (Feb. 20, 2004). Report of the APA Task Force on Advertising and Children.

[22] Ofcom. (Nov. 2016). Children and parents: Media use and attitudes report; Graff, S., Kunkel, D., & Mermin, S. E. (2012). Government can regulate food advertising to children because cognitive research shows that it is inherently misleading. *Health Affairs 2*, 392–398; Valkenburg, P. M., & Cantor, J. (2001). The development of a child into a consumer. *Journal of Applied Developmental Psychology, 22(1)*, 61–72. https://doi.org/10.1016/S0193-3973(00)00066-6; Carter, O. B. J., et al. (March 2011). Children's understanding of the selling versus persuasive intent of junk food advertising: Implications for regulation. *Social Science & Medicine, Volume 72, Issue 6*, 962–968.

[23] Daems, K., De Pelsmacker, P., & Moons, I. (Nov. 17, 2017). Advertisers' perceptions regarding the ethical appropriateness of new advertising formats aimed at minors. *Journal of Marketing Communications.*

[24] Children's Commissioner. (Nov. 8, 2018). *Who knows what about me?*; Livingstone, S. (2019). YouTube's child viewers may struggle to recognise adverts in videos from 'virtual play dates.' London, U.K.: London School of Economics.

[25] Anonymous. (May 8–13, 2021). "They see you're a girl if you pick a pink robot with a skirt": How children conceptualize data processing and digital privacy risks. *CHI '21: ACM CHI Conference on Human Factors in Computing Systems*; academics studying children's interactions with apps have found that "some thought everyone received the same ads," or perhaps the same ads but not at the exact same time, while some thought "certain ads would be shown for the same video at the same time, similar to TV ads."

[26] Zhao, J., Wang, G., Dally, C., Slovak, P., Childs, J. E., Van Kleek, M., & Shadbolt, N. (May 2019). "I make up a silly name": Understanding children's perception of privacy risks online. *CHI Conference on Human Factors in Computing Systems Proceedings 2019*, p. 2.

[27] Gibbs, S. (July 8, 2015). Women less likely to be shown ads for high-paid jobs on Google, study shows. *The Guardian.*

[28] Richardson, R., & Miller, M. L. (Jan. 13, 2021). The higher education industry is embracing predatory and discriminatory student data practices. Slate.

themselves back, too: When young people know all their activities are being monitored by surveillance technologies, they appear less likely to engage in critical thinking, political activity, or questioning of authority.[29] Targeted ads can expose aspects of teens' lives they would prefer to share on their own terms, and the consequences of being inadvertently outed and exposed can be worse for kids without legal autonomy. A child may not appreciate ads for LGTBQ+ resources showing up on a shared device, but any ads that reflect sexual interests, drugs, and professional interests can affect kids' privacy. A pregnant teenager, for example, likely would prefer to break the news to her family in a way that does not include a targeted mailer.[30]

Furthermore, industry groups insist that behavioral ads are more relevant and personalized, but this ignores the fact that this is often a one-way street. Kids aren't choosing the ads they want; companies are data-mining kids to figure out what to target them with. Often, what companies think kids want is inappropriate or even dangerous. Kids watching videos on YouTube have been subjected to inappropriate ads that include violence, sexual content, and politics.[31] Kids may be profiled as gamers, impulsive purchasers, or anxious oversharers—and then unfairly targeted by ads that encourage more of these things. Facebook, for example, has categorized hundreds of thousands of kids as "interested in" gambling and alcohol.[32] And Facebook also got into hot water when it was revealed that employees had told advertisers they could identify when teens and other young people were feeling "stressed," "defeated," "overwhelmed," "anxious," "nervous," "stupid," "silly," "useless," and "a failure".[33] Kids who are anxious or have low self-esteem don't need to be shown more makeup tutorials, offered a coffee pick-me-up, or otherwise commercially manipulated.

Kids who are anxious or have low self-esteem don't need to be shown more makeup tutorials, offered a coffee pick-me-up, or otherwise commercially manipulated.

Behaviorally targeted ads provide limited benefits to most companies

It is a common expression in advertising circles that half the money spent on advertising is wasted, but no one knows which half.[34] This is a serious concern in online advertising, where fraud to generate ad impressions, clicks, or conversions is rampant. Studies have suggested that $1 out of every $3 spent on online advertising goes to fake traffic and automated bots.[35] The companies that make their money from talking about how effective targeted advertising is have routinely been found to be exaggerating their capabilities. Facebook admitted to inflating video viewership metrics, and Comscore, which measures online advertising, was charged with falsely

[29] Brown, D. H., & Pecora, N. (2014). Online data privacy as a children's media right: Toward global policy principles. *Journal of Children and Media, 8(2)*, 201–207.
[30] Duhigg, C. (Feb. 16, 2012). How companies learn your secrets. *The New York Times*.
[31] Radesky, J. S., Schaller, A., Yeo, S. L., Weeks, H. M., & Robb, M. B. (Nov. 2020). Young kids and YouTube: How ads, toys, and games dominate viewing. Retrieved from Common Sense website: https://d2e111jq13me73.cloudfront.net/sites/default/files/uploads/research/2020_youngkidsyoutube-report_final-release_forweb.pdf
[32] Hern, A., and Ledegaard, F. H. (Oct. 9, 2019). Children 'interested in' gambling and alcohol, according to Facebook. *The Guardian*.
[33] Levin, S. (May 1, 2017). Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless'. *The Guardian*.
[34] Franks, J. U. (Aug. 25, 2017). We now know which half of advertising is wasted. HuffPost News.
[35] Vranica, S. (March 23, 2014). A 'crisis' in online ads: One-third of traffic is bogus. *The Wall Street Journal*.

reporting its revenue and misreporting customer numbers.[36] This is on top of the adtech intermediaries that also take a cut from each ad transaction—Google and Facebook alone take up 60% of all online ad revenue. This "adtech tax" means that publishers end up receiving only 30 to 40 cents of every dollar spent to advertise on their sites.[37]

A 2019 study by researchers at three U.S. universities found that ad publishers' revenues increased by only 4 percent when cookies were available compared to when cookies were disabled, meaning that using personal data to target ads increased revenue by an average of just $0.00008 per ad. A former digital advertising strategist for the *New York Times* has argued that behavioral advertizing "has been completely overhyped in its value for publishers from the day it was first invented."[38]

Industry groups constantly argue that privacy rules and any restriction on behavioral advertising will eliminate "ad-supported free" services without detailing what this means.[39] This orthodoxy ensures that other models of supporting healthier digital content are afforded no opportunity to flourish; it also has made cash-strapped local media perpetually more dependent upon this business model, to its detriment.

Changes are coming—and overdue—for adtech

Behaviorally targeted ads displaced contextual advertising, which could be poised to make a comeback because of new privacy regulations and the decision of companies like Apple and Mozilla to restrict tracking tools.[40] Adtech companies often avoid discussing the value of contextual advertising compared to behavioral ads. Because contextual ads involve displaying ads based on a website's content or an app's target demographic, they do not rely on personal profiling and therefore do not require or justify intensive data collection and tracking as a means of getting "free" content.

After the EU's General Data Protection Regulation went into effect, the *New York Times* cut off advertising exchanges in Europe and kept growing ad revenue for itself. The paper's vice president of advertising data called privacy laws that reduce reliance on third-party ad targeting a "win-win-win" for publishers, advertisers, and, importantly, consumers.[41] Similarly, the *Washington Post* committed to "[going] beyond cookie-based ad targeting and [matching] ads to people without being 'creepy.'"[42] It is true that big publishers like the *Times* and the *Post* are better positioned to rely on their own internal data to understand viewer demographics, but smaller publishers' and services' reliance on adtech has created an experience that is neither user-friendly nor economically sustainable.

---

[36] Robertson, A. (Sept. 24, 2019). Comscore, the internet's traffic judge, settles fraud charges for $5 million.
[37] News Media Alliance. (Nov. 16, 2020). Big Tech says publishers keep majority of ad revenue, but experience suggests otherwise.
[38] Hagey, K. (May 29, 2019). Behavioral ad targeting not paying off for publishers, study suggests. *The Wall Street Journal*.
[39] Prieto, L. (Oct. 22, 2019). NAI consumer survey on privacy and digital advertising. Network Advertising Initiative.
[40] Dillon, G. (Feb. 22, 2021). What's old is new again: The return of contextual targeting. ExchangeWire.
[41] Trimmer, K. (Feb. 22, 2019). Third-party data is a bad habit we need to kick. AdExchanger.
[42] Moses, L. (March 7, 2019). The Washington Post is trying to go beyond cookie-based ad targeting and match ads to people without being 'creepy'. *Business Insider*.

Contextual advertising has been shown to be more cost effective than behaviorally targeted ads,[43] and reducing reliance on adtech also can have benefits to internet users: After *USA Today* removed adtech software from its European websites, the site not only had less surreptitious tracking but it also loaded faster. *USA Today*'s U.S. website is 5.5 megabytes in size and includes more than 800 ad-related requests for information involving 188 different domains. In contrast, the EU-facing site is less than half a megabyte in size and contains no third-party tracking.[44]

The justifications for behavioral ad tracking are growing increasingly thin. And privacy worries are forcing massive changes in the entire online advertising ecosystem. Apple has made headlines by announcing that updates to iOS will require companies to ask permission before they track iPhone users.[45] At the same time, Google has switched on a new technology in its Chrome browser known as Federated Learning of Cohorts, or FLoC, which actually has nothing to do with federated learning but instead hides individual browsing activity "in the crowd" of similar cohorts.[46] FLoC is no panacea, and some have argued that it could raise more privacy problems than it solves.[47] It is conceivable that children themselves could be lumped together into their own FLoC cohort. Still, the message is growing even from within the industry itself that adtech has to change.

Against this backdrop, lawmakers are finally beginning to propose outright bans on behaviorally targeted ads[48] and to question whether third-party trackers are malware.[49] Laws like the California Privacy Rights Act promise to legally enshrine technical measures like the Global Privacy Control; tools like the Global Privacy Control let individuals easily exercise their privacy rights with multiple companies at once by turning off targeted advertising and data sharing through a universal technical signal.

Efforts to curb behavioral advertising to kids have international support. For example, Ireland has proposed that "organisations should, in general, avoid profiling children for marketing purposes, due to their particular vulnerability and susceptibility to behavioural advertising." Ireland, like the U.K., asks companies to prioritize the best interests of the child, and the Irish Data Protection Commission flatly stated that it does not consider behavioral ads or auto-suggestions based on profiling to be in the best interests of children.[50] Limiting behavioral ad targeting and tracking also is consistent with the U.N. Convention on the Rights of the Child General Comment No. 25, which notes that behavioral marketing and profiling are "becoming routine" and that "[s]uch practices may lead to arbitrary or unlawful interference with children's right to privacy; they may have adverse consequences on children, which can continue to affect them at later stages of their lives."[51]

---

[43] GumGum (Sept. 6, 2020). Understanding contextual relevance and efficiency.

[44] Jerome, J. (April 1, 2019). The GDPR's impact on innovation should not be overstated. Center for Democracy and Technology.

[45] Levy, D. Speaking up for small business. Facebook.

[46] Bindra, C. (Jan. 25, 2021). Building a privacy-first future for web advertising. Google.

[47] Cyphers, B. (March 3, 2021). Google's FLoC is a terrible idea. Electronic Frontier Foundation.

[48] Davis, W. (March 25, 2021). Lawmakers ready bill to ban 'surveillance advertising'. Media Post.

[49] U.S. Senate Committee on the Judiciary hearing (April 21, 2021). Antitrust applied: Examining competition in app stores; in questions directed to a Google representative, Senator Jon Ossoff (D-Ga.) suggested that mobile apps were reliant on software development kits, or SDKs, that were effectively malware. SDKs are tools that app developers can use to quickly include all sorts of functionality in apps without having to code things themselves, but because SDKs are operated by third parties, they can be a prime source of data leakage or otherwise aggressively exfiltrate user's information from an app.

[50] Data Protection Commission. (Dec. 2020). Children front and centre: Fundamentals for a child-oriented approach to data processing.

[51] United Nations Human Rights Office of the High Commissioner. General comment on children's rights in relation to the digital environment, No. 25. U.N. Committee on the Rights of the Child.

Recommendations for future policy

Targeted ads and the privacy-invasive behaviors that flow from this type of marketing may be more trouble than they're worth, particularly when kids are the target audience. Common Sense believes that lawmakers and industry experts can work together to reduce and ultimately eliminate targeted ads directed at children. Self-restraint and regulation are ultimately necessary.

- We recommend that Congress prohibit the behavioral tracking and targeting of kids. Privacy legislation should flat-out prohibit behaviorally targeted ads for kids under 13, and ideally for any person a digital service believes to be under 18. At the very least, the default should be that behavioral ad targeting is off for teens and their informed permission is required to opt in to targeted advertising. State laws like the California Privacy Rights Act and international frameworks already are moving in this direction.

- We recommend that the Federal Trade Commission provide more guidance and, importantly, undertake more enforcement activities targeting online advertising. It can update, codify, and enforce advertising guidelines including those regarding endorsements and disclosures, and incorporate any learnings about how targeted ads can unfairly discriminate when it comes to children and teens and undermine the Children's Online Privacy Protection Act through its ongoing 6(b) study into tech companies and social media platforms.[52] It should put out guidance regarding behavioral ads and where their use is unfair to children and teens, including, if necessary, by commencing a rulemaking.

- We recommend that companies be honest about when they have kids on their services and use first- and third-party technologies that respect the best interests of children and teens. Companies should be proactive about thinking about when kids could be engaging with their products and services and not incorporate privacy-invasive third-party trackers into children's apps.[53]

Conclusion

Behavioral ads provide questionable financial benefits to businesses, and they harm impressionable kids. Young people do not want them and are defenseless against advanced targeting and profiling. Now is the time for companies, and policymakers, to advance advertising business models that better serve kids and families.

[52] Fair, L. (Dec. 4, 2020). FTC issues 6(b) orders to social media and video streaming services.
[53] Lieff Cabraser Heimann & Bernstein, LLP. (April 13, 2021). Settlement receives final approval in Disney/Viacom/Kiloo child privacy violations lawsuit.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BEN RAY LUJÁN TO ANGELA J. CAMPBELL

Senator Luján wrote:

In your testimony, you make the point that overuse of digital media among children has been associated with mental health problems, poor nutrition, problems in school, cyberbullying, and online sexual abuse. Facebook has justified the creation of Instagram for Kids by pointing to the fact that a majority of kids 8 to 13 are already using social media. Instead of addressing the problem, Facebook has decided to capitalize on the problem. Instagram for Kids won't reduce the number of young children using social media. Instead, by design it will encourage them to start using it at younger and younger ages.

Question. What implications does lowering the age at which children are first exposed to social media have on their development?

Answer. Thank you for asking this very important question. Lowering the age at which children are first exposed to social media would harm children's development and well-being.

The Children's Online Privacy Protection Act of 1998 (COPPA), and the FTC rules implementing COPPA, are intended to prevent the collection, use and disclosure of personal information from children under age 13 except in very limited circumstances.[1] Consequently, most social media platforms have terms of service stating that they are intended only for persons aged 13 or older. These platforms were designed for adults to maximize engagement, such as likes, shares, and comments. They were not been designed to serve the best interests of children.

Nonetheless, many children under age 13 use social media platforms designed for adults such as Instagram, YouTube, TikTok, and Snapchat, as well as gaming and other platforms that allow communication among strangers.[2] Children can easily evade getting parental consent simply by giving a false birthdate.[3] Creating Instagram for Children will not solve this problem. Underage children currently using Instagram are unlikely to switch to children's accounts.[4] Rather, the effect will be to encourage the creation of new accounts by even more younger children.

While COPPA would require that Instagram for Kids give direct notice of its privacy practices to parents and obtain advance verifiable consent from parents, this does not protect young children from the many risks presented by social media. Privacy policies are not required to disclose the risks,[5] and parents are often unaware of them. Most parents do not have the time or ability to research and assess the risks, or to monitor all their children's online activities. And even if parents do everything reasonably possible to protect their child, they still may not succeed. For example, the *Wall Street Journal* describes a case in which a parent read Roblox's parental guide and set up an account specifically for a child under 13, but the child

---

[1] 15 USC §§ 6501–6505; 16 CFR Part 312.

[2] Nellie Bowles and Michael H. Keller, *Video Games and Online Chats are 'Hunting Ground' for Sexual Predators,* NY Times, Dec. 7, 2019 (describing how criminals, often posing as children, strike up conversations with and gradually build trust to dupe children into sharing sexually explicit photos and videos of themselves using platforms extremely popular with children such as Fortnite, Minecraft and Roblox), *https://www.nytimes.com/interactive/2019/12/07/us/video-games-child-sex-abuse.html. See also* Julie Jargon, *Roblox Struggles With Sexual Content. It Hopes a Ratings System Will Address the Problem,* Wall St. J., Apr. 17, 2021 (reporting that Fortnite has 32.6 million daily users, more than half of which are under 13, and in some Fortnite games "players' blocky avatars simulate sex, engage in raunchy talk and 'date' other avatars.")

[3] For example, after the United States filed a complaint alleging TikTok violated COPPA by permitting children under 13 to use the service without parental notice and consent and TikTok signed a consent agreement requiring it to comply with COPPA, TikTok created accounts for U.S. users under 13 that allowed children to make videos using their phones but not to share them with others. A subsequent investigation by Campaign for a Commercial-Free Childhood found that many children under 13 were continuing to post videos of themselves on TikTok without their parents' knowledge or consent. *Advocates Say TikTok in Contempt of Court Order,* May 14, 2020, *https://commercialfreechildhood.org/tiktok-pr/. See also* Raymond Zhong and Sheera Frenkel, *A Third of TikTok's U.S. Users May Be 14 or Under, Raising Safety Questions,* NY Times (Aug. 14, 2020), *https://www.nytimes.com/2020/08/14/technology/tiktok-underage-users-ftc.html.*

[4] Katie Canales, *40 percent of kids under 13 already use Instagram and some are experiencing abuse and sexual solicitation, a report finds, as the tech giant considers building an Instagram app for kids,* Business Insider (May 13, 2021). Similarly, YouTube's creation of YouTube Kids had limited if any effect on the large number of children using YouTube, but did lead to new accounts for the youngest children.

[5] 16 CFR § 312.4 generally requires operators only to make reasonable efforts to give parents notice of their practices with regard to the collection, use and disclosure of personal information collected from children.

was still exposed to inappropriate sexual content.[6] Moreover, an online service designed for children could have a design flaw allowing young children to circumvent parental controls. This actually happened with Facebook's Messenger Kids in 2019, when a design flaw enabled children to chat with strangers.[7]

Using social media poses many risks for children. The very purpose of social media is for individuals to share information with others. Social media provides opportunities to exchange information with anyone online. Generally, parents and society protect young children by limiting their contacts with unknown persons and by providing schools and other environments designed to promote healthy development.

Social media undermines these efforts by allowing unknown individuals to communicate directly with children and companies to use, sell and make available to third-parties information collected from children. Often, such information is personally identifiable. It may include names, physical or e-mail addresses, geolocation, telephone numbers, photographs, videos or audio recordings. Social media networks and other digital platforms constantly track what users do online, which can provide a wealth of information on such sensitive topics as mood, likes and dislikes, political opinions, medical concerns, and sexual orientation. Advertisers can use this information to target manipulative advertisements. Photographs posted online can be "scraped" and used for facial recognition by almost anyone.[8] Personal data can be bought and sold, combined, and mined to reveal all sorts of insights about individuals, which can be used for harmful purposes.

As discussed below, a large body of research, mostly involving teens, associates social media use with a variety of negative outcomes including depression and anxiety, cyberbullying, sleep problems, unhealthy body images, and sexual abuse. Given that younger children are still developing their cognitive, social, and emotional skills, they are even more vulnerable to these risks than adolescents.

Children are even more vulnerable than teens to the risks posed by social media

During early and mid-childhood, children develop basic motor, cognitive, and social skills, which are crucial for further development. Cognitive functions include memory, attention, visual-spatial, and executive functions, while complex cognitive processes include: thinking (abstract, cause and effect, creative thinking, and planning) and language functions. The most intensive development of all components of executive functions, especially cognitive flexibility, happens at school age, usually between 7 and 12 years of age.[9] Until children have developed these capacities, they simply are not able understand the risks of using social media. For example, children between the ages of 4 and 10 show limited understanding of digital privacy concepts, such as what companies might know about them.[10]

Threats to children's developing self-esteem

Social media usage by children may undermine their developing sense of self-esteem. Self-esteem is shaped not only by a child's own perceptions and expectations, but also by the perceptions and expectations of significant people in her life—how she is thought of and treated by parents, teachers and friends.[11] Social media generally, and Instagram in particular, with its focus on photo sharing and appearance, are unsuitable for children in the crucial stages of developing their sense of self. Social media platforms encourage users to upload videos and photos and to make and receive likes and comments from other users. This can lead young people to obses-

---

[6] *Roblox Struggles with Sexual Content, supra* n.2.

[7] Russell Brandom, *Facebook Design Flaw Let Thousands of Kids Join Chats with Unauthorized Users,* TheVerge, July 22, 2019, *https://www.theverge.com/2019/7/22/20706250/facebook-messenger-kids-bug-chat-appunauthorized-adults.*

[8] *E.g.,* Drew Harwell, *This facial recognition website can turn anyone into a cop—or a stalker,* Washington Post, May 14, 2021, *https://www.washingtonpost.com/technology/2021/05/14/pim eyes-facial-recognition-search-secrecy/.*

[9] Ilona Bidzan-Bluma and Malgorzata Lipowska, *Physical Activity and Cognitive Functioning of Children: A Systematic Review,* In.t J. Enviornal. Res. Public Health, April 2018, *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5923842/.*

[10] 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,* Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, May 2021, *https://dl.acm.org/doi/pdf/10.1145/3411764.3445333?casa_token=oHIzkQDpdJgAAAAA:QdkV TdxOyCV6I-6ACT9rp7AaKn-Q1F7f_ugKb7tsQ-HGnNuRv7OPYId9M7ZUMLB56X4Fbet088RMw.*

[11] American Academy of Pediatrics, Helping Your Child Develop A Healthy Sense of Self Esteem, *https://www.healthychildren.org/English/ages-stages/ gradeschool/Pages/Helping-Your-Child-Develop-A-Healthy-Sense-of-Self-Esteem.aspx.*

sively check for reactions to their posts, or to post even more outrageous or inappropriate content to garner more reactions.

In addition, editing photos and videos and using filters to present an idealized version of oneself is the norm on Instagram and many other social media platforms. The constant pressure to compare themselves to others is likely to have detrimental effects on children. As clinical psychologist Bethany Cook notes:

> social media—especially Instagram—allows us control over what we share with the outside world. Many of us prefer to show our "best light" and/or a "filtered" version of our life. When children see this version of life and then compare it to their own, it often creates feelings of anger, frustrations, resentment, depression, and stress they don't know how to emotionally process on their own. It doesn't matter if you explain to them "it's all fake," because the part of their brain needed to fully comprehend and understand this concept isn't fully developed until around the age 21–25.[12]

Increased risk of depression and anxiety

Depression and anxiety among children and teens have increased in recent years.[13] Increased depressive symptoms and rising suicide rates have been correlated with increasing use of smart phones and social media. For example, a 2020 review of "evidence from a variety of cross-sectional, longitudinal and empirical studies implicate smartphone and social media use in the increase in mental distress, self-injurious behaviour and suicidality among youth."[14] Another study analyzed three large data sets (two from the U.S. and one from the UK) and found that "Adolescents using digital media an hour or less a day reported the highest levels of well-being, and those using digital media 5 or more hours a day reported the lowest levels of well-being."[15] A longitudinal study of 7,596 UK children aged 10 to 15 found that that "high use of social media was significantly associated with a decrease in happiness, and that girls, in particular, experienced the largest decline in happiness and were more likely to have a worsening trajectory over time.[16]

In 2017, the Royal Society for Public Health (RSPH) surveyed 1,479 14–24 year-olds in the UK about the five most popular social media platforms: Facebook, Instagram, Snapchat, Twitter and YouTube. Those surveyed reported that four of the five social media platforms actually made their feelings of anxiety worse.[17] The survey concluded that Instagram was the worst social media platform for youth mental health. A U.S. organization, BARK, analyzed more than 2.1 billion messages in 2020, including texts, YouTube, e-mails and over thirty different social media networks. It found that "41.4 percent of tweens and 66.6 percent of teens were involved in a self-harm/suicidal situation," which included anything from text messages

---

[12] Murphy Moroney, *What Parents Should Know About Instagram's New App For Kids Under 13,* POPSUGAR Family, March 19, 2021, *https://www.popsugar.com/node/48227541.*

[13] Centers for Disease Control and Prevention, Data and Statistics on Children's Mental Health, *https://www.cdc.gov/childrensmentalhealth/ data.html. See also* Elia Abi-Jaoude *et al., Smartphones, Social Media Use and Youth Mental Health,* 192(6) CMAJ, 136–141 (2020); *https://www.cmaj.ca/content/cmaj/192/6/E136.full.pdf.* Boys' depressive symptoms increased by 21 percent from 2012 to 2015, while depressive symptoms for girls increased by 50 percent—more than twice as much. The rise in suicide, too, is more pronounced among girls. Although the rate increased for both sexes, three times as many 12-to-14-year-old girls killed themselves in 2015 as in 2007, compared with twice as many boys. The suicide rate is still higher for boys, in part because they use more-lethal methods, but girls are beginning to close the gap. Jean M. Twenge, *Have Smartphones Destroyed a Generation?,* The Atlantic, Sept. 2017.

[14] Elia Abi-Jaoude *et al., Smartphones, Social Media Use and Youth Mental Health,* 192(6) CMAJ, 136–141 (2020); *https://www.cmaj.ca/content/cmaj/192/6/E136.full.pdf.* Also found there is a dose–response relationship, and the effects appear to be greatest among girls.

[15] Jean M. Twenge and W. Keith Campbell, *Media Use Is Linked to Lower Psychological Well-Being: Evidence from Three Datasets,* Psychiatric Quarterly 90, no. 2 (June 1, 2019): 311–31.

[16] Liz Twigg, *et al., Is social media use associated with children's well-being? Results from the UK Household Longitudinal Study.* Betul Keles, *et al., A systematic review: the influence of social media on depression, anxiety and psychological distress in adolescents,* International Journal of Adolescence and Youth (2019) (systematic review of found that the amount of time spent using social media, activity (such as number of social media accounts, frequency of checking messages), investment in social media, and social media addiction were prominent risk factors for depression, anxiety and psychological distress in adolescents), tandfonline.com/doi/full/10.1080/02673843.2019.1590851?scroll=top&needAccess=true. Royal Society for Public Health, #*StatusofMind* (May 2017), at 8 (summarizing growing evidence linking social media use and depression in young people), *https://www.rsph.org.uk/our-work/campaigns/status-of-mind.html.*

[17] #*StatusofMind* at 18–23.

about cutting to an e-mail draft of a suicide note.[18] It also found that the top 2 platforms flagged for severe suicidal ideation were Twitter and Instagram.[19]

Cyberbullying

Many mental health problems of youth are related to cyberbullying. As explained by the RSPH:

> Bullying during childhood is a major risk factor for a number of issues including mental health, education and social relationships, with long-lasting effects often carried right through to adulthood. The rise of social media has meant that children and young people are in almost constant contact with each other. The school day is filled with face-to-face interaction, and time at home is filled with contact through social media platforms. There is very little time spent uncontactable for today's young people. While much of this interaction is positive, it also presents opportunities for bullies to continue their abuse even when not physically near an individual.[20]

The RSPH survey found that 7 in 10 young people had experienced cyberbullying, with 37 percent of young people saying they experienced cyberbullying on a high-frequency basis. Similarly, a survey of U.S. teens by the Pew Research Center, found that 59 percent of U.S. teens reported being bullied on social media.[21] Cyberbullying is particularly rampant on Instagram.[22]

Detrimental Impacts on Sleep

Social media use also affects sleep, which is related to mental health. As the RSPH notes,

> Poor mental health can lead to poor sleep and poor sleep can lead to states of poor mental health. Sleep is particularly important for teens and young adults due to this being a key time for development. The brain is not fully developed until a person is well into their twenties and thirties. Sleep is essential for allowing us to function properly during waking hours and teens need around 1–2 hours more sleep every night than adults. Poor sleep is linked to a wide range of both physical and mental health conditions in adults including high blood pressure, diabetes, obesity, heart attack, stroke and depression.[23]

Numerous studies show that social media usage can decrease the quantity and quality of sleep. For example, a survey of 11,361 teens aged 13–15 in the UK found that "heavy use of screen media was associated with shorter sleep duration, longer sleep latency, and more mid-sleep awakenings." These associations were strongest for teens using screen media to engage in social media or to use the internet."[24]

Unhealthy body image

Body image is a concern for many young people, especially girls. The RSPH found that 9 in 10 teenage girls are unhappy with their body.[25] A study of girls in middle and high school found that frequently posting on Facebook was "significantly correlated with weight dissatisfaction, drive for thinness, thin ideal internalization and

---

[18] BARK, Annual Report: 2020 Research on children and technology, *https://www.bark.us/annual-report.*

[19] *Id.*

[20] #*StatusofMind* at 11 (footnotes omitted).

[21] *A Majority of Teens Have Experienced Some Form of Cyberbullying,* Pew Research Center: Internet, Science & Tech (blog), Sept. 27, 2018, *https://www.pewresearch.org/internet/ 2018/09/27/a-majority-of-teens-haveexperienced-some-form-of-cyberbullying/.*

[22] Taylor Lorenz, *Teens Are Being Bullied 'Constantly' on Instagram,* The Atlantic, Oct. 10, 2018, *https://www.theatlantic.com/technology/archive/2018/10/teens-face-relentless-bullying-instagram/572164/.* Taylor Lorenz, *Teens Are Spamming Instagram to Fight an Apparent Network of Child Porn,* The Atlantic, Jan. 8, 2019, *https://www.theatlantic.com/technology/archive/2019/01/meme-accounts-are-fighting-child-porninstagram/579730/.*

[23] #*StatusofMind* at 9 (footnotes omitted).

[24] Garrett Hisler, *et al., Associations between screen time and short sleep duration among adolescents varies by media type: evidence from a cohort study,* 66 Sleep Medicine 92 (2020). *See also* Heather C. Woods and Holly Scott, H. #*Sleepyteens: Social media use in adolescence is associated with poor sleep quality, anxiety, depression and low self-esteem.* 51 J. of Adolescence 41 (2016)((finding that "adolescents who used social media more—both overall and at night—and those who were more emotionally invested in social media experienced poorer sleep quality, lower self-esteem and higher levels of anxiety and depression); Ben Carter *et al., A Systematic Review and Meta-Analysis,* 170 JAMA Pediatrics 1202 (Dec. 1, 2016); Russell M. Viner, *et al., Roles of cyberbullying, sleep, and physical activity in mediating the effects of social media use on mental health and wellbeing among young people in England: a secondary analysis of longitudinal data,* 3 The Lancet Child & Adolescent Health 685 (2019).

[25] #*StatusofMind* at 10, & n. 35.

self-objectification."[26] Interviews with children aged 11–16 in three European countries revealed that adolescent girls felt pressured to post sexualized selfies as a means of generating attention and social acceptance from their peers.[27] A survey of close to 300 girls between the ages of 12 and 16 in Singapore found that "girls place high importance on both the number of likes and positive comments they receive. The findings also indicate that teenage girls with low self-esteem attach higher importance to peer feedback, and the level of such importance is positively associated with depressed mood."[28] Relatedly, most social media platforms have communities that promote anorexia and other eating disorders.[29]

Online sexual abuse

Another serious risk to young people on social media is exposure to child sexual abuse materials. Social media platforms including Instagram are rife with images and videos portraying child sexual abuse. In 2019, nearly 70 million such images and videos were reported to the National Center for Missing and Exploited children (NCMEC), representing an increase of more than 50 percent from 2018.[30] Of reports filed with NCMEC by US-based electronic service providers, the vast proportion came from Facebook, which owns Instagram.[31]

Not only are children exposed to sexual images on social media, but they are often solicited to engage in sexual interactions. While different studies may use different terminology, there is no doubt that many young people are groomed by adults online for sexual purposes.[32] NCMEC, for example, reports receiving 19,174 "online enticement reports" in 2019, and almost twice that number (37,872) in 2020.[33] ECPAT International uses the term sexual extortion or "sextortion," which it defines as

> a process whereby children or young people are coerced into continuing to produce sexual material and/or told to perform distressing acts under threat of exposure to others of the material. In some instances, the abuse spirals so out

---

[26] Evelyn P. Meier and James Gray, *Facebook Photo Activity Associated with Body Image Disturbance in Adolescent Girls,* 17 Cyberpsychology, behavior and social networking (2014).

[27] Giovanna Mascheroni, *et al., "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).

[28] Pengxiang Li, *et al., "Likes" as KPI; An examination of teenage girls' perspective on peer feedback on Instagram and its influence on coping response,* 35 Telematics and Informatics 1994 (2018). *See also* Trudy Hui Hui Chua and Leanne Chang, *Follow Me and like My Beautiful Selfies: Singapore Teenage Girls' Engagement in Self-Presentation and Peer Comparison on Social Media,* 55 Computers in Human Behavior 190 (2016) (finding teenage girls negotiate their self-presentation efforts to achieve the standards of beauty projected by their peers, use the tools, likes and followers, to measure and grant peer approval of physical beauty, and their actions are driven by the desire to gain attention, validation, and recognition, which ultimately link to issues of insecurity and low self-esteem).

[29] *E.g.* Atte Oksanen, *et al., Proanorexia Communities on Social Media,* 137 Pediatrics 1(Jan. 2016); Fabrizio Bert et al, *Risks and Threats of Social Media Website: Twitter and the Proana Movement,* 19 Cyberpsychology, Behavior, and Social Networking (2016).

[30] Gabriel J.X. Dance and Michael H. Keller, *Tech Companies Detect a Surge in Online Videos of Child Sexual Abuse,* NY Times, Feb. 7, 2020, *https://www.nytimes.com/2020/02/07/us/online-child-sexual-abuse.html.* This number dipped only slightly to 65.4 million in 2020. NCMEC, By the Numbers, *https://www.missingkids.org/gethelpnow/cybertipline#bythenumbers.*

[31] In 2019, Facebook made 15,884,511 reports out of a total of 16,836,694. In 2020, Facebook made 20,307,216 out of 21,447,786. *Id. See also* Tom Porter, *Facebook Reported More than 20 Million Child Sexual Abuse Images in 2020, More than Any Other Company,* Business Insider, Feb. 26, 2021, *https://www.businessinsider.com/facebook-instagramreport-20-million-child-sexual-abuse-images-2021-2.* It is not clear why the numbers reported by Facebook are so much higher than other companies such as Google and TikTok. It may be that Facebook does a better job of finding and reporting child sex abuse images. Katherine Hamilton, *Facebook reports majority of child sex abuse images in 2020, data shows,* June 7, 2021, *https://nbc-2.com/features/tech/2021/03/01/facebook-reports-majority-of-child-sex-abuse-images-in-2020-data-shows/.*

[32] For example, ECPAT International, a global network of more than 100 civil society organizations working to end the sexual exploitation of children, has identified five different types of online child sexual exploitation—child sexual abuse material (CSAM); online grooming; sexting; sexual extortion and live online child sexual abuse. *Online Child Sexual Exploitation: A Common Understanding,* May 2017, *https://www.ecpat.org/wp-content/uploads/2017/05/SECO-Booklet_ebook-1.pdf.*

[33] NCMEC explains that "Online Enticement involves an individual communicating with someone believed to be a child via the Internet with the intent to commit a sexual offense or abduction. This is a broad category of online exploitation and includes sextortion, in which a child is being groomed to take sexually explicit images and/or ultimately meet face-to-face with someone for sexual purposes, or to engage in a sexual conversation online or, in some instances, to sell/trade the child's sexual images. This type of victimization takes place across every platform; social media, messaging apps, gaming platforms, etc." *Online Enticement, https://www.missingkids.org/theissues/onlineenticement.*

of control that victims have attempted to self-harm or commit suicide as the only way of escaping it.[34]

Thorn, a nonprofit organization that develops new technologies to combat online child sexual abuse, conducted surveys of victims of sextortion in 2015 and 2017. Its 2017 survey of more than 2,000 victims aged 13 to 25 found that nearly a quarter were 13 years or younger when the sextortion occurred.[35] It also found that younger victims were more likely to experience sextortion from online offenders (as opposed to someone they knew offline) and to be threatened for explicit imagery.[36] In another survey conducted in 2020 of 1,000 minors aged 9–17, Thorn found that a third reported having had an online sexual interaction.[37] The majority of these harmful interactions took place on popular platforms such as Snapchat (26 percent), Instagram (26 percent), YouTube (19 percent), TikTok (18 percent), and Messenger (18 percent).[38]

Online sexual abuse can have significant and lasting effects. Victims of child abuse are more likely to suffer from mental health problems, attempt and commit suicide, and develop alcohol or drug dependencies. These outcomes impact every aspect of a child's life, including their ability to develop into productive adults."[39]

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. BEN RAY LUJÁN TO SERGE EGELMAN, PH.D.

Implications of security and privacy breaches in a platform designed for kids. Facebook says that Instagram for Kids can be designed to protect children online. But given their history, there is reason to be concerned. In a recent open letter, the National Association of Attorneys General cited Facebook's long history of failing to protect the safety and privacy of children online. Facebook has built privacy controls before, but design flaws have repeatedly exposed their users to unsafe and vulnerable situations.

Question. What are the implications of security and privacy breaches in a product designed exclusively for children?

Answer. When the privacy and security of children's products are breached, there are numerous implications. One concern is unauthorized access to the collected identifiable data. For example, child predators may see these services as attractive targets; they may break into children's accounts in order to perform reconnaissance on potential victims. Another concern is the public disclosure of the data in the event of a data breach or due to indiscriminate sharing of the data with third parties (*e.g.,* anyone may be able to buy the data from data brokers). In this manner, children's data may still end up in the hands of child predators, who then may use it to identify and locate victims, and then use their knowledge of each child's interests to lure them.

---

[34] *A Common Understanding,* supra n. 32.

[35] *Sextortion, Summary Finding from a 2017 survey of 2,097 survivors* at 6. *https://www.thorn.org/wp-content/uploads/2019/12/Sextortion_Wave2Report_121919.pdf.*

[36] *Id.* at 7.

[37] Thorn, *Responding to Online Threats: Minors' Perspectives on Disclosing Reporting and Blocking,* May 2021, *https://info.thorn.org/hubfs/Research/Responding%20to%20Online%20Threats_2021-Full-Report.pdf.* Response options coded as an "online sexual interaction" included: being asked for a nude image or video, being asked to go "on cam" with a nude or sexually explicit stream, being sent a nude photo or video, or being sent sexually explicit messages. *Id.* at 8–10.

[38] *Id.* at 13. Similarly, a review of UK police reports of 1,220 offenses of sexual communications with a child over a 3-month period (Apr.1 to June 30, 2020), found that Instagram was involved in more offenses (37 percent) than any other platform, while Facebook-owned apps (including Instagram) were used in 51 percent of reported cases. NSPCC, *Instagram most recorded platform used in child grooming crimes during lockdown,* Nov. 13, 2020, *https://www.nspcc.org.uk/about-us/news-opinion/2020/instagram-grooming-crimes-children-lockdown/. See also* BARK, *Annual Report: 2020 Research on children and technology, https://www.bark.us/annual-report* (identifying top 5 apps or platforms flagged for sexual content, severe suicidal ideation, severe depression, body image concerns, bullying, hate speech, and violence).

[39] In addition, the impacts of online child sexual exploitation and abuse extend into the economics sphere, including expenditures by health care systems that treat children for short-and long-term injuries; costs associated with treating psychological and behavioral problems, costs incurred by social welfare systems involved with monitoring, preventing and responding to cases of violence against children; and costs associated with finding, persecuting and jailing perpetrators of child violence through the criminal justice system. Global Partnership to End Violence against Children, *Child Online Safety,* at 5, *https://www.end-violence.org/sites/default/files/paragraphs/download/Online%20Child%20Safety%20175.pdf.*

The data being used by child predators to identify and lure potential abuse victims represents an extreme, albeit feasible, use of this type of data. A much more likely scenario is the situation where a non-custodial parent (or someone else known to the child) breaks into a child's account to plan a kidnapping or coordinate prohibited communication. Incidents occur all the time where account compromise and an unaccountable data broker ecosystem enable domestic abusers to stalk and abuse their victims, there is no reason to believe that these same tactics will not be used against children.

A related concern is that because proving identity is very difficult on the Internet—it is considered an open problem and is why social engineering attacks are so prevalent (*e.g.,* phishing)—it is difficult for services targeted at children to guarantee that their users are actually children, and not adults pretending to be children. I am not aware of a good solution to this problem: even if the service could somehow prove that a child initially created an account, they cannot easily prove that that child continues to control the account (as opposed to it being controlled by an adult). Thus, even if the accounts of child users are not compromised by predators directly, child users may still be targeted by child predators who use accounts to pose as children so that they can identify victims, communicate with them, and/or arrange to meet them. There is not a good technological solution to this problem, which continues to plague many online platforms.