United States of America
Federal Trade Commission

The FTC's Role in Supporting Online Safety

Christine S. Wilson*
Commissioner, U.S. Federal Trade Commission

Remarks at the Family Online Safety Institute

Washington, DC
November 21, 2019

---

* The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission or any other Commissioner. Many thanks to my Attorney Advisor, Nina Frant, and my Paralegal, Olivia Berry, for assisting in the preparation of these remarks.

I. INTRODUCTION

Good morning! Many thanks to the Family Online Safety Institute ("FOSI") and Emma Morris for inviting me here today, and to Patricia Vance for the kind introduction. I appreciate the opportunity to share my thoughts on online safety. Before I begin, though, I must give the standard disclaimer. The views I express today are my own, and do not necessarily reflect the views of the U.S. Federal Trade Commission or any other Commissioner.

I'd like to start by stating the obvious – an online presence is integral to so many aspects of our lives. We connect with friends, family, and interest groups. We shop for clothes, household items, cars, and houses. Small business owners can reach far-flung customers, enabling them to earn a livelihood not possible with a local customer base. Students can attend online classes and earn college degrees without ever stepping foot in a physical classroom. Information on every conceivable topic is at our fingertips – and so are movies, songs, books, and endless other ways to increase our knowledge and broaden our horizons.

As both a mother and an aunt, I have experienced firsthand the opportunities that the internet can provide to kids. My older daughter has always loved to cook and, as a vegan in high school, was able to find innovative and nutritious recipes online. My niece, who dreams of owning a horse rescue operation, has conducted research online regarding floor plans for barns that optimize the health of resident horses. And my younger daughter has long had a knack for computer programming, robotics, and building things. In middle school, after researching similar projects online, she built a prototype of a basketball tracking system using an Xbox Kinect sensor to track and record the movement of a ball around a basketball court.

So technology can be constructive and horizon broadening. Like money or power, though, technology can be used for both great advancements and bad acts. Thus, the unfortunate

truth is that life online comes with risk. The news is filled with stories of social media bullying. We've all heard the tragic stories of teens committing suicide after severe episodes of cyberbullying.[1] Predators use chatrooms and social media to establish contact with children and arrange in-person meetings.[2] And Backpage was accused of hosting child trafficking ads; its CEO ultimately pled guilty last year to facilitating prostitution and money laundering.[3]

I remind the audience of these stories not to stoke fear, but rather to stress that as active citizens concerned about the safety of children, we have to remain vigilant about confronting the brutal fact that the internet can be a dangerous place. We as parents and policymakers must confront these risks and do what we can to minimize them so that our children can become the next generation of leaders, which will require them to be fully literate digital citizens. It is not an easy task – I had my fair share of discussions with my children about the dangers of the internet. We discussed whether they could join various social media platforms, play connected video games with online chat rooms, or create a YouTube channel. Aside from a brief encounter with cyberbullying, though, I am grateful that the other dark possibilities that lurk on the internet have not directly affected my children or me.

And to be clear, most of the online dangers that I have referenced fall outside the jurisdiction of the FTC. But they highlight the need for parents to take an active role in

---

[1] Emily S. Rueb, *A Teenager Killed Himself After Being Outed as Bisexual. His Family Wants Justice*, N.Y. TIMES, Sept. 30, 2019, https://www.nytimes.com/2019/09/30/us/channing-smith-suicide-bisexual-tennessee.html; Jamiel Lynch, *Police accuse two students, age 12, of cyberbullying in suicide*, CNN, Jan. 24, 2018, 3:36 PM, https://www.cnn.com/2018/01/23/us/florida-cyberstalking-charges-girl-suicide/index.html. The Pew Research Center also issued a report on cyberbullying. Monica Anderson, *A majority of Teens Have Experienced Some Form of Cyberbullying*, PEW CHARITABLE TRUST (2018), https://www.pewresearch.org/internet/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/.

[2] Christine Elgersma, *The Facts About Online Predators Every Parent Should Know*, COMMON SENSE MEDIA (July 25, 2017), https://www.commonsensemedia.org/blog/the-facts-about-online-predators-every-parent-should-know; Janis Wolak et al., *Online Predators: Myth versus Reality*, NEW ENG. J. PUB. POL'Y, available at http://scholarworks.umb.edu/cgi/viewcontent.cgi?article=1646&context=nejpp.

[3] Tom Jackman, *Backpage CEO Carl Ferrer pleads guilty in three states, agrees to testify against other website officials*, WASH. POST, Apr. 13, 2018, https://www.washingtonpost.com/news/true-crime/wp/2018/04/13/backpage-ceo-carl-ferrer-pleads-guilty-in-three-states-agrees-to-testify-against-other-website-officials/.

educating their children about the risks, as well as the benefits, of an online presence. And, as you know, the FTC supports parents in keeping kids safe online both through its educational materials and through its enforcement of the Children's Online Privacy Protection Act ("COPPA") and our COPPA Rule.

First, I'd like to highlight some of the FTC's recent COPPA cases. Next, I'd like to talk about the FTC's ongoing review of the COPPA Rule. This summer, the FTC announced a request for comments on the Rule. The comment period is open until December 9, 2019, so I want to spend a few minutes highlighting issues on which your input will be invaluable to the FTC.

Finally, I want to talk about the limits of COPPA. COPPA does not speak to a number of online dangers like stalking, grooming, or cyber-bullying. So I want to conclude my remarks by spending a few minutes talking about how the FTC has taken steps to promote online safety outside the COPPA arena.

II. RECENT COPPA CASES

At its core, COPPA and the corresponding Rule require operators of commercial websites, apps, and other online services to provide notice and obtain parental consent before collecting personal information from children under the age of 13. The Rule ensures that parents and children have truthful information about a company's privacy and security practices when making decisions about which apps and websites to use.

Within the Rule's relatively narrow scope, the FTC has built a rigorous enforcement program to protect children's privacy. To date, the FTC has brought more than 30 COPPA cases

against a variety of entities, including app developers, online review sites, retailers, and network advertisers.[4]

One recent COPPA enforcement action that has garnered significant attention involves YouTube (and its parent company Google).[5] YouTube claimed to be a general audience site, but as the complaint alleges, the company knew many of its channels – like channels operated by toy companies – were "directed to children."[6] Our complaint also alleged that YouTube collected personal information to track viewers over time and across websites – in order to target advertising to children without first getting parental consent. The case makes clear that, if general audience sites gain knowledge that user-generated content on their platforms is directed at children, they must comply with COPPA.

The YouTube settlement also speaks to obligations of content creators under COPPA.[7] When content creators generate programming directed to children, the law requires them to get verifiable parental consent before engaging in behavioral advertising on their own sites or through their own apps. The same obligations arise when those content creators are hosted by third-party platforms. In other words, if content creators have child-directed channels on YouTube, they must comply with COPPA.

Last week YouTube formally announced its plan to have content creators identify videos or channels that are made for kids. I am aware of consternation on the part of content creators, thanks in large part to a tidal wave of tweets I've received. Content creators have expressed

[4] *See Business Center: Children's Privacy*, FED. TRADE COMM'N, available at https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=246.
[5] *See* Compl., FTC v. Google LLC and YouTube, LLC, No. 1:19-cv-02642 (D.D.C. filed Sept. 6, 2019), available at https://www.ftc.gov/enforcement/cases-proceedings/172-3083/google-llc-youtube-llc.
[6] 16 C.F.R. § 312.2 (defining "Web site or online service directed to children").
[7] Stipulated Order for Permanent Injunction and Civil Penalty Judgment, FTC v. Google LLC and YouTube, LLC, No. 1:19-cv-02642 (D.D.C. filed Sept. 10, 2019), available at https://www.ftc.gov/system/files/documents/cases/172_3083_youtube_coppa_consent_order_signed.pdf.

worries about potential fines, lost revenue, and disabled popular features like comments and end screens that drive user-engagement. Many content creators also have expressed significant confusion about whether content would be classified as "directed to children." The FTC looks at a variety of factors to determine whether a site or service is directed to children under 13.[8] Although the assessment is admittedly subjective, the agency is not trying to hide the ball when determining whether content is child-directed. We have a number of guidance documents available on our website, including our business compliance guides that provide examples and scenarios to assist with COPPA compliance. [9]

Another recent Commission matter targeted Musical.ly (now TikTok). The case directly addresses the various factors the Commission considers when determining whether a website or service meets the test for being "directed to children."[10] The Musical.ly app met several of those factors because it contained child-oriented activities, music appealing to children, and child celebrities. The Commission alleged that a large percentage of its users were children, and in fact, many of them self-identified as under 13 in their profile bios.[11] The complaint further

[8] Factors the FTC considers include the subject matter of the site or service (*e.g.*, educational), visual and audio content (*e.g*., unicorns, nursery rhymes), the use of animated characters or other child-oriented activities and incentives, the age of models, the presence of child celebrities or celebrities who appeal to kids, ads on the site or service that are directed to children, and other reliable evidence about the age of the actual or intended audience (*e.g.*, complexity of language, viewer information). *See* 16 C.F.R. § 312.2 (definition of "Web site or online service directed to children").

[9] *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance (last visited Nov. 21, 2019); *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Web%20sites%20and%20online (last visited Nov. 21, 2019); *see also* Kristin Cohen, *YouTube channel owners: Is your content directed to children?*, FED. TRADE COMM'N BUSINESS BLOG (Nov. 22, 2019, 12:56 PM), https://www.ftc.gov/news-events/blogs/business-blog/2019/11/youtube-channel-owners-your-content-directed-children.

[10] Compl., U.S. v. Musical.ly, et al., No. 2:19-cv-1439 (C.D. Cal. filed Mar. 27, 2019), https://www.ftc.gov/system/files/documents/cases/musical.ly_complaint_ecf_2-27-19.pdf.

[11] Separate from our complaint, FTC action was timely because a number of news outlets reported a large community of adult users on TikTok soliciting nude photos from children. The Musical.ly app allowed strangers to view other users within a 50-mile radius of their location and directly message them, without providing notice or obtaining parental consent. Katey Roshetko, *Online predators use ten app Tik Tok to solicit children*, WDJB7, Mar.

explains that TikTok had several indications that children were using the app, because the company:

- Provided parents with guidance about their children's use of the app;
- Received complaints from parents that their children created accounts without their knowledge; and
- Sent emails to several popular users asking them to edit their profile descriptions to indicate that a parent or adult talent manager was running their accounts.

Given that the Musical.ly app was directed to children under the factors set out in the Rule and the company failed to seek parental consent before collecting personal information from users under the age of 13, the FTC rightly pursued this COPPA case.

Following the YouTube and Musical.ly cases, companies and creators should carefully evaluate their sites, services, and content to determine whether they are in fact directed to children. And companies should have processes in place to obtain parental consent and revise collection practices if they gain actual knowledge that they have collected personal information from children. If a company determines that it has actual knowledge that a user is under 13, it must seek verifiable parental consent or delete any previously collected personal information. Additionally, companies must honor requests from parents to delete information collected from their children under 13.

III. FTC'S ONGOING REVIEW OF THE COPPA RULE

While our recent enforcement efforts illustrate the important role COPPA plays in protecting children's online privacy, we all know that the privacy risks that children and parents

6, 2019, https://www.wdbj7.com/content/news/Parents-warned-online-predators-often-use-popular-teen-app-Tik-Tok-to-lure-children-506752631.html#:~:targetText=ROANOKE%2C%20Va.,beating%20out%20Instagram%20and%20Facebook.

face evolve as quickly as technology. The FTC has worked to keep COPPA current by amending the Rule to address innovations that affect children's privacy. When the Rule was drafted in 1998, children primarily accessed the internet through family desktop computers. By 2013, though, children used phones to access the internet. Phones made it easy for children to share pictures, videos, and precise geolocation data. So revisions to the Rule made clear that COPPA applied to mobile apps. The 2013 Rule amendments also updated the definition of "personal information" to include geolocation information as well as photos, videos, and audio files that contain a child's image or voice. These revisions were designed to address changing technology and sought to keep the Rule relevant and effective.

Although the FTC's last COPPA Rule Review ended in 2013, the Commission is conducting its ten-year review early because of growing questions about the Rule's application to the educational technology sector, to voice-enabled connected devices, and to general audience platforms that host third-party child-directed content. I'd like to touch briefly on each of these topics.

The first topic on which the FTC is seeking comment pertains to educational technology, or "EdTech." Classroom apps are mining data and conducting analytics to evaluate student engagement and help teachers structure learning environments. As EdTech gets more sophisticated, it is collecting larger volumes of sensitive data to help drive analytics – including biometric, academic, behavioral, and disciplinary data. Captured information may also include student web browsing history, geolocation data, and IP addresses.

In the Statement of Basis and Purpose to the 1999 COPPA Rule, the Commission noted that the Rule "does not preclude schools from acting as intermediaries between operators and

schools in the notice and consent process, or from serving as the parents' agent in the process."[12] But COPPA does not specifically address how schools can obtain verifiable parental consent.

Although I am aware of the debate about the wisdom of EdTech in the classroom, the FTC is not passing judgment on the value of EdTech. Instead, we are exploring whether and how the Rule should address parental consent for EdTech vendors that collect the personal information of students. Your insights will help the FTC assess whether we should consider a specific exception to parental consent for the use of EdTech in schools, and the proper limitations of that exception.

The FTC is also requesting comment on whether exceptions to parental consent are warranted for the collection of audio files as a replacement for text. Our 2017 Enforcement Policy Statement made clear that the practice of collecting audio files that contain a child's voice, immediately converting the audio to text, and deleting the file containing the voice did not run afoul of COPPA. Questions have been raised, however, about whether operators should be able to de-identify audio files and keep them to improve products. Questions have also been raised about whether companies can safeguard de-identified audio files from re-identification. So again, I encourage operators and parents to submit comments on this issue.

Finally, the Commission also is considering important issues raised in our recent enforcement actions. Should the Rule be amended to better address websites and online services that may not meet the current definition of "website or online service directed to children," but that have a large number of child users? Are there circumstances in which general audience platforms with third-party, child-directed content should be able to rebut the presumption that all users interacting with that content are children?

[12] Children's Online Privacy Protection Rule, 65 Fed. Reg. 59,888, 59,903 (Nov. 3, 1999).

The current Rule review is an important opportunity to hear from parents, companies, and policy organizations like FOSI about what more can and should be done to protect children's privacy. I would like to emphasize that this Rule review is not an attempt to weaken privacy protections for children, but instead to make certain that the Rule continues to serve the goals Congress articulated in 1998.

IV. THE LIMITS OF COPPA

To function effectively in today's world, our children must be equipped to navigate life online in a safe and informed way. Through COPPA enforcement, the FTC is able to advance this goal by addressing some very serious practices that impact children's privacy. But the statutory authority granted to the FTC under COPPA is well defined and relatively narrow. The purpose of COPPA is to put parents in the driver's seat. But as I mentioned at the outset of my remarks, the risks to children on the internet extend beyond data collection.

In an article that FOSI posted in October 2018, Parven Kaur cautioned that parents need to remember that any social media platform can be a source of cyberbullying and a ground for sexual predators.[13] We saw this phenomenon with TikTok and with some apps I will discuss in a minute. To enable our children to take full advantage of the opportunities offered by an online presence in a safe and informed way, we parents have a key role to play.

Like FOSI, the FTC also offers resources for online safety. Our consumer information website, available at consumer.ftc.gov, includes a number of resources for protecting kids online. Another FTC resource, Net Cetera, gives parents, teachers, and other adults who spend time with

[13] Praven Kaur, *What Families Need to Know About TikTok*, FAM. ONLINE SAFETY INST. (Oct. 9, 2018), https://www.fosi.org/good-digital-parenting/what-families-need-know-about-tiktok/

children guidance on how to launch conversations about social networking, privacy, computer security, and cyberbullying.[14]

While COPPA focuses on parental consent, the FTC's Section 5 authority allows the agency to police a wider cross-section of dangerous online behavior. Section 5 of the FTC Act, dating back to 1914, prohibits "unfair or deceptive business practices in or affecting commerce."[15] We have recently used this old but flexible and broad statute to reach new technologies that facilitate twenty-first century versions of harms like digital stalking,[16] revenge porn,[17] and invasions of people's homes through web cameras.[18] Let me give you two examples.

First, the FTC recently took quick action with respect to a Ukraine-based company, Wildec, that created three dating apps that allowed adults to find and communicate with children. When this came to our attention, we sent a letter to Wildec – and simultaneously to Google and Apple – asserting potential COPPA and Section 5 violations. These apps collected users' birthdates, email addresses, photographs, and real-time location data. They claimed to prohibit users under the age of 13, but FTC staff was able to search for other users by age and location to find nearby users as young as 12 years old. Several individuals also reportedly face criminal charges for contacting or attempting to contact minors using Wildec's apps. Thankfully, Google and Apple swiftly removed the apps from their app stores.

---

[14] *Net Cetera: Chatting with Kids About Being Online*, FED. TRADE COMM'N (2014), https://www.consumer.ftc.gov/articles/pdf-0001-netcetera_0.pdf.
[15] 15 U.S.C. §45.
[16] Compl., Retina-X Studios, LLC, No. 172-3118 (filed Oct. 22, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3118/retina-x-studios-llc-matter.
[17] Compl., FTC v. EMP Media, Inc. also d/b/a Myex.com, No. 2:18-CV-00035 (D. Nev. filed Jan. 9, 2018), https://www.ftc.gov/enforcement/cases-proceedings/162- 3052/emp-media-inc-myexcom.
[18] Compl., TRENDnet, Inc., No. 122-3090 (filed Feb. 7, 2014), https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.

Second, and just last month, the FTC brought its first case against stalkerware – spyware that secretly monitors another person's smartphone. The FTC is aware that many parents monitor their children's devices, and the use of spyware by parents to monitor children is a legitimate use of such technology. But Retina-X and its owner James Johns developed three mobile device apps that served as stalking apps.[19] According to the FTC's complaint, the apps shared detailed information about smartphone activities like call history, text messages, photos, and GPS locations without a user's permission. And the apps provided purchasers with instructions on how to remove the app's icon from appearing on the mobile device's screen, meaning the device user was unaware that he or she was being monitored. Further, the apps were uploaded through rooting or jailbreaking devices.[20] According to the complaint, the purported use of the monitoring products and services for employment or child-monitoring purposes was pretext. Employers or parents would not typically jailbreak or root phones to install apps, particularly when many other monitoring products are available in the marketplace that do not require installation steps that can expose phones to security vulnerabilities or likely invalidate a phone's warranties. These apps were promoted as tools to monitor mobile devices used by children, but in the wrong hands, they enabled domestic abusers to track targets' physical movements and online activities. Based on all of these facts, we concluded that Section 5 was violated.

The FTC's Section 5 authority cannot reach every danger facing kids on the internet today. But, when a company knows that its products and/or services present a substantial risk of harm, especially physical harm, the FTC may be able to bring a case alleging an unfair practice.

[19] Compl., Retina-X Studios, LLC, No. 172-3118 (filed Oct. 22, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3118/retina-x-studios-llc-matter.
[20] Jailbreaking typically entails actions to bypass various restrictions implemented by the operating system and/or the manufacturer of mobile devices.

During our COPPA workshop in October, I heard one attendee say that the FTC needs to make the internet safe for kids. That is a tall order for one federal agency in one of almost 200 countries around the world, almost all of which have active contributors to the internet. I also submit to you that while the FTC can help erect guardrails, keeping kids safe online is a job that begins at home.

V. CONCLUSION

Parenting in the digital age is challenging and requires a continuous assessment of benefits and risks. Technology can be a wonderful resource, connecting children with infinite sources of history and culture. But to fully reap the rewards of online spaces, parents must acknowledge the risks and take steps to mitigate potential harms through monitoring, education, and communication. I look forward to continuing to partner with FOSI and the other organizations in the audience today. The FTC remains committed to protecting children's privacy and working to secure children's safety. Together we can help make sure that parents have the tools they need to protect their families and make informed choices about their kids and the internet. Thank you for having me here today and I look forward to continuing the conversation.