



UNITED STATES OF AMERICA
Federal Trade Commission

“Taking Care: The American Approach to Protecting Children’s Privacy”

Prepared Remarks of Commissioner Noah Joshua Phillips*

**Family Online Safety Institute
2018 Annual Conference**

**Washington, DC
November 15, 2018**

Good morning. I am pleased to be here today to commemorate the twentieth anniversary of the enactment of the Children’s Online Privacy Protection Act, or “COPPA.” On October 21, 1998, Congress enacted COPPA to prohibit unfair or deceptive acts or practices in connection with the collection, use, or disclosure of personally identifiable information from children on the Internet. As you are aware, in that statute, Congress gave the Federal Trade Commission the responsibility for promulgating, and enforcing, the COPPA Rule. As an FTC commissioner, I am here today in my professional capacity to discuss children’s privacy and the role my agency plays in protecting that privacy. However, as a parent of three young children, my interest in children’s privacy is also personal.

Not a week goes by when I don’t catch one or more of my kids giggling as they ask Siri any number of inappropriate questions. Sometimes, I cannot help but giggle myself. But I see them interacting with technology in new and different ways,

* The views expressed below are my own and do not necessarily reflect those of the Commission or of any other Commissioner.

without the will inherent in how adults interact with the world. And I am aware that, as time goes by, they will encounter child-directed technologies that may collect information about them. Even though COPPA was enacted twenty years ago, discussion about the American approach to protecting children’s privacy could not be more timely or relevant. As we speak, our country is grappling with the challenge of consumer privacy more broadly. I believe that our experience with COPPA – from its enactment, to its implementation, and to its enforcement – can help inform and guide these other policy discussions.

The FTC’s involvement with children’s online privacy – and indeed online privacy more generally – dates back to 1995, when the FTC began holding workshops and Commission hearings to examine industry guidelines governing information practices online. In early 1998, the FTC conducted a comprehensive online survey of the information practices of commercial websites, including 212 websites directed to children.¹ That survey found that almost 90% of children’s websites at the time were collecting personal information from and about children, including through registration pages, user surveys, online contests, electronic pen pal programs, and guest books. Children also had unfettered access to chat rooms and electronic bulletin boards, and any personal information posted there was publicly accessible to anyone on the Internet. At the same time, only 54% of the child-directed websites surveyed provided any sort of statement about their information collection practices, 23% told children to get parental consent before

¹ Fed. Trade Comm’n, *Privacy Online: A Report to Congress* 31-38 (1998), <https://www.ftc.gov/reports/privacy-online-report-congress>.

providing personal information, and a mere 1% obtained parental permission before collecting information from children. As you can imagine, these findings raised questions not only about children’s privacy, but also about their physical safety.

Congress acted quickly, with then Representative, now Senator, Edward Markey and Senator Richard Bryan introducing bills in their respective chambers. Senator Bryan marveled at how swiftly Congress acted, pointing out that, “[i]n a matter of only a few months since Chairman McCain and I introduced this bill last summer, we have been able to achieve a remarkable consensus.”² He credited this “in large part to the recognition by a wide range of constituencies that the issue is an important one that requires prompt attention by Congress.”³ He also recognized that the consensus was due to the input of a broad range of stakeholders, noting that revisions to the original bill “were worked out carefully with the participation of the marketing and online industries, the Federal Trade Commission, privacy groups, and first amendment organizations.”⁴ Senator Bryan then elaborated on the goals of the legislation: to enhance parental involvement in children’s online activities to protect both their privacy and safety; to maintain the security of the personally identifiable information collected from children online; and to protect children’s privacy by limiting the collection of personal information from children without their parent’s consent.⁵ He concluded by pointing out that “[t]he legislation accomplishes these goals in a manner that preserves the interactivity of children’s

² 144 CONG. REC. S11,657 (daily ed. Oct. 7, 1998) (statement of Sen. Bryan).

³ *Id.*

⁴ *Id.*

⁵ *Id.*

experience on the Internet and preserves children’s access to information in this rich and valuable medium.”⁶

I stress this Congressional history for a couple of reasons. First, it illustrates the important role of Congress in making the tough choices when it comes to privacy and the tradeoffs inherent in privacy regulation. Congress, working with its constituencies, recognized a need for legislation to protect children’s privacy and it drafted a bill. The bill, however, needed additional work. Congress did not just give the FTC carte blanche to do what it thought best; instead, Congress itself worked with all stakeholders to revise and then pass legislation that effectuated its intent. For example, one of the tough issues with which Congress grappled was the age of children to be covered by COPPA. The initial legislative draft of COPPA defined a child as an “individual under the age of 16”⁷ and anticipated providing some protection to children to the age of 17. The bill proposed requiring verifiable parent consent for children under the age of 13, which the current law also requires. However, the bill also had proposed requiring websites to “use reasonable efforts to provide the parents with notice and an opportunity to prevent or curtail the collection or use of personal information collected from children over the age of 12 and under the age of 17”.⁸ As commentators have pointed out, Congress ultimately recognized that this requirement had the potential to chill older minors in pursuit of

⁶ *Id.*

⁷ S. 2326, 105th Cong. § 2 (as introduced, July 17, 1998).

⁸ *Id.* § 3.

information, and removed the requirement in recognition of the difficult First Amendment questions it would raise.⁹

Second, Senator Bryan’s remarks also highlight another important concept: the American privacy framework is built upon identifying risks and then designing a solution that balances competing interests. This requires evaluating the sensitivity of the information involved and the potential harms that would result from its collection, use or disclosure, and then creating a solution that will limit these harms while still allowing appropriate use of even sensitive information. With COPPA, rather than trying to protect children’s privacy and safety by enacting draconian legislation that could severely limit children’s experience on the Internet, Congress instead created a comprehensive, yet flexible, framework to protect both children’s privacy and children’s ability to access interactive content on the Internet.

One way that this statutory flexibility has been born out is with respect to the requirements relating to “verifiable parental consent.” The statute defined verifiable parental consent as – and I am paraphrasing here -- any reasonable effort, taking into consideration available technology, to ensure that the parent receives notice and authorizes the collection, use, and disclosure of the child’s personal information prior to any collection.¹⁰ In including the modifier – “taking

⁹ Berin Szoka & Adam Thierer, *COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech*, 16 PROGRESS ON POINT 1, 4-5 (2009), https://www.ftc.gov/sites/default/files/documents/public_comments/2010-childrens-online-privacy-protection-act-rule-review-547597-00052%C2%A0/547597-00052-54901.pdf (citing the Congressional testimony of Deirdre Mulligan, Center for Democracy and Technology).

¹⁰ 15 U.S.C. § 6501 (9).

into consideration available technology” – Congress recognized that there was no perfect mechanism for obtaining parental consent, and that the cost of requiring even a close-to-perfect mechanism might not be justified in all cases. In drafting the first iteration of the COPPA Rule, FTC staff recognized that the cost of a technologically rigorous mechanism could sometimes outweigh its benefits, especially if there was less risk associated with the collection and use of the child’s information.¹¹ Accordingly, in cases where the child’s information would be shared with third parties, or disclosed on the Internet, the Rule required more stringent methods of verifiable parental consent. However, in cases where the website was not going to share or disclose the child’s information, the Rule provided for less costly methods of obtaining consent. This was described as a “sliding scale mechanism” for providing parental consent.

This sliding scale was intended to be a temporary option, because staff and other stakeholders believed the development of technological solutions would lower the cost of obtaining parental consent.¹² However, such mechanisms are not readily available at a reasonable cost, and the FTC ultimately made the sliding scale mechanism permanent.¹³ Importantly, they were able to engage in this cost-benefit analysis because Congress drafted the COPPA statute with this consideration in mind.

This statutory flexibility has been important in other ways as well. In 1998, when Congress enacted COPPA, technology looked quite different. At that time, a

¹¹ Children’s Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,899-902 (Nov. 3, 1999).

¹² *Id.* at 59,902.

¹³ *Compare* 16 C.F.R. § 312.5 (2005), *with* 16 C.F.R. § 312.5 (2013).

major concern was that children were providing their personal information through website registration forms and surveys, or posting contact information on “electronic bulletin boards.” The first three cases the FTC brought under the COPPA Rule are illustrative. The *GirlsLife.com* website targeted girls aged 9 to 14, and offered features such as online articles and advice columns, contests, and pen-pal opportunities.¹⁴ Partnering with *BigMailbox.com* and *Looksmart*, the *GirlsLife* website also offered children free email accounts and online message boards. In these three cases, the FTC alleged that the defendants each collected children’s full names and home addresses, email addresses and telephone numbers. None of these websites posted privacy policies that complied with COPPA or obtained the required consent from parents before collecting this information.

In 1998, social networks, smartphones, geolocation, and static IP addresses were barely on the horizon. Despite these developments, the flexibility of the COPPA statutory framework has ensured that the COPPA Rule continues to protect children in all these new scenarios. In 2005, the FTC conducted a review of the Rule, but decided to retain it unchanged.¹⁵ However, in 2010, the FTC recognized that changes to the online environment over the prior five years, including children’s use of mobile technology to access the Internet, warranted another look.¹⁶ The FTC reached out to stakeholders to determine whether the Rule’s definition of

¹⁴ FTC Press Release, *FTC Announces Settlements with Web Sites That Collected Children’s Personal Data Without Parental Permission* (Apr. 19, 2001), <https://www.ftc.gov/news-events/press-releases/2001/04/ftc-announces-settlements-web-sites-collected-childrens-personal>.

¹⁵ Children’s Online Privacy Protection Rule, 71 Fed. Reg. 13,247 (Mar. 15, 2006).

¹⁶ Request for Public Comment on the Federal Trade Commission’s Implementation of the Children’s Online Privacy Protection Rule, 75 Fed. Reg. 17,089 (Apr. 5, 2010).

“Internet” applied to mobile communications, interactive television, interactive gaming, and similar activities. FTC staff also asked for comment on whether the Rule’s definition of “personal information” should include other items of information, such as persistent IP addresses, mobile geolocation information, or information collected in connection with online behavioral advertising.¹⁷

In December 2012, after a thorough notice and comment process, the FTC announced amendments to the COPPA Rule, which addressed changes to the technology landscape.¹⁸ Among other things, the amended Rule 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. The amended Rule was expanded to cover persistent identifiers that can recognize users over time and across different websites and online services, such as IP addresses and mobile device IDs. The amendments also made clear that the COPPA Rule covered child-directed sites or services that integrate outside services, such as plug-ins or advertising networks, that collect personal information from its visitors. In addition, the amendments also clarified that if plug-ins or ad networks have actual knowledge that they are collecting personal information from a child-directed website or online service, they must also comply with the Rule.

Recent cases against app developers illustrate how the COPPA Rule continues to protect children’s privacy. In *LAI Systems* and *Retro Dreamer*,

¹⁷ *Id.* at 17,090.

¹⁸ Children’s Online Privacy Protection Rule, 78 Fed. Reg. 3,972 (Jan. 17, 2013); *See also* FTC Press Release, *FTC Strengthens Kids’ Privacy, Gives Parents Greater Control Over Their Information By Amending Childrens Online Privacy Protection Rule* (Dec. 19, 2012), <https://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over>.

defendants created a number of apps directed to children, such as, My Cake Shop, My Pizza Shop, Marley the Talking Dog, Happy Pudding Jump, Sneezies, Wash the Dishes, and Cat Basket. The FTC alleged that these app developers allowed third-party advertisers to collect personal information from children in the form of persistent identifiers. The app developers violated COPPA when they failed to inform the ad networks that these were child-directed apps, and did not provide notice or get consent from children’s parents for collecting and using the information.¹⁹ In *VTech Electronics*, the FTC brought its first children’s privacy case involving Internet-connected toys, alleging that the company violated COPPA by collecting personal information from children without providing direct notice and obtaining their parent’s consent, and failing to take reasonable steps to secure the data it collected.²⁰

The United States has a proud tradition of considering and protecting privacy, dating back to the drafting of the Constitution itself.²¹ Congress developed our statutory scheme for consumer privacy over the last half a century, enacting statutes that cover a range of sensitive information, including children’s personal information,²² information collected and used by consumer reporting agencies,²³

¹⁹ FTC Press Release, *Two App Developers Settle FTC Charges They Violated Children’s Online Privacy Protection Act* (Dec. 17, 2015), <https://www.ftc.gov/news-events/press-releases/2015/12/two-app-developers-settle-ftc-charges-they-violated-childrens>.

²⁰ FTC Press Release, *Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children’s Privacy Law and the FTC Act* (Jan. 8, 2018), <https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated>.

²¹ U.S. CONST. amend. IV.

²² Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. § 6501 *et seq.* and 16 C.F.R. § 312.

²³ Fair Credit Reporting Act (“FCRA”), 15 U.S.C. § 1681 *et seq.*

financial information,²⁴ health information,²⁵ student education records,²⁶ telephonic,²⁷ and electronic communications.²⁸ Congress also has legislated on if, and when telemarketers can intrude upon the privacy of your home. The FTC backstops these more specific, risk-based, rules with its authority to protect consumers from deception and unfair practices, a flexible model that can react to new privacy risks, technologies, and market developments.

This American privacy framework recognizes the tradeoffs at issue in the privacy debate, balancing privacy interests with innovation and competition, and protecting most the data considered to pose the greatest risk if shared or otherwise misused. This approach – like any other – is not infallible, and re-evaluation and recalibration may, at times, be warranted in light of changed circumstances. Nevertheless, our risk-based framework has permitted innovation, competition and economic growth for decades.

There are those who would tell you that we need to avoid using personal data at all costs, especially when it comes to children. I believe that is an overly dystopian view that focuses on the possibility of harm and entirely discounts the potential promise of technologies. Instead, our approach should be one of taking care when it comes to data and children. For example, e-learning platforms can use

²⁴ Gramm-Leach-Bliley (“GLB”) Act, 15 U.S.C. § 6801 *et seq.*; Financial Privacy Rule, 16 C.F.R. § 313; Standards for Safeguarding Customer Information, 16 C.F.R. § 314.

²⁵ Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 42 U.S.C. and 29 U.S.C.).

²⁶ Family Educational Rights and Privacy Act of 1974 (“FERPA”), 20 U.S.C. § 1232g.

²⁷ Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C.).

²⁸ Electronic Communications Privacy Act of 1986 (“ECPA”), Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

data to support teachers, students, and parents creating customized lesson plans or dynamically focusing on areas an individual student finds challenging. However, to do that, they may need to use personal data. We should balance the risks, and help children, parents, and educators understand those risks. At the same time, we also must recognize where data support new technologies that serve important public goods.

I would like to leave you with a few parting thoughts. First, the American approach to privacy is grounded on Congressional deliberation and action. Congress is equipped to make the fundamental value judgments that laws protecting privacy inevitably require. Weighing innovation or economic growth against protecting children is a hard choice, as may be deciding how to punish wrongs that may not cause clearly calculable harms; but making these tough decisions is what the people elect their representatives to do. They do not elect Federal Trade Commissioners.

Second, and therefore, when Congress takes action and enacts a privacy statute, it is our job faithfully to execute congressional will and enforce that law. This is important in all contexts, but I would argue it is especially important when protecting the privacy of children. As a Federal Trade Commissioner, I consider it crucial that we continue to investigate businesses' practices as they relate to children's privacy, and that we enforce this law as Congress intended. At the new FTC, COPPA enforcement ought to be a signature feature of our American privacy regime.

Third, I believe the FTC's experience with the COPPA statute and the COPPA Rule can play a valuable role in informing our nation's policy-making on privacy going forward. COPPA is a deliberately paternalistic statute, because it deals with children; so it is not necessarily a model for broader privacy legislation. But, as I discussed earlier, despite the fact that COPPA is twenty years old, its more flexible approach to protecting children's privacy has been a critical component in its continuing success and effectiveness. In considering the best ways to protect consumer privacy, we should learn from our experience with COPPA.

Fourth and finally, on the general privacy front, we are going to have a big national debate because there are real policy disagreements. However, if Congress and the Administration choose a particular path forward, the Federal Trade Commission is committed to undertaking the role it is given.

* * *