

Hope M. Babcock
Angela J. Campbell
Directors
Andrew Jay Schwartzman
Benton Senior Counselor
James T. Graves
Ariel Nelson
Adam Riedel
Staff Attorneys

600 New Jersey Avenue NW
Suite 312
Washington, DC 20001-2075
Telephone: 202-662-9535
Fax: 202-662-9634



GEORGETOWN LAW
INSTITUTE FOR PUBLIC REPRESENTATION

October 3, 2018

VIA E-MAIL

Donald S. Clark, Secretary of the Commission
Andrew Smith, Director, Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

Dear Mr. Clark and Mr. Smith,

Campaign for a Commercial-Free Childhood (CCFC), by its counsel, the Institute for Public Representation, together with the undersigned organizations, write to ask the Federal Trade Commission to investigate and take enforcement action against Facebook for violating the Children’s Online Privacy Protection Act. Facebook’s messaging application for children under 13, Messenger Kids, is the first major social media platform designed specifically for young children—as young as five years of age. Messenger Kids violates COPPA by collecting personal information from children without obtaining verifiable parental consent or providing parents with clear and complete disclosures of Facebook’s data practices.

In January 2018, CCFC asked Facebook to discontinue its Messenger Kids app because of the developmental risks it poses to children. In a letter signed by 118 public health advocates and organizations, CCFC said “a growing body of research demonstrates that excessive use of digital devices and social media is harmful to children and teens, making it very likely this new app will undermine children’s healthy development.”¹

In addition to these serious child development issues, Facebook’s Messenger Kids application does not comply with COPPA—despite Facebook’s claims to the contrary.² Messenger Kids

¹ Letter from Campaign for a Commercial-Free Childhood *et al.* to Mark Zuckerberg, Facebook (Jan. 30, 2018), <http://www.commercialfreechildhood.org/sites/default/files/develop-generate/gaw/FBMessengerKids.pdf>.

² Messenger Kids, <https://messengerkids.com/> (“Is Messenger Kids COPPA compliant? Yes. Messenger Kids is designed to be compliant with important child privacy laws like the Children’s Online Privacy Protection Act (COPPA).”).

falls short of COPPA compliance in at least two ways. First, the application’s parental consent mechanism is not reasonably calculated to ensure that the person providing consent is the child’s parent—or even an adult. In fact, it employs a mechanism similar to one that the FTC has previously rejected. Second, Facebook’s privacy notice for Messenger Kids³ is confusing and incomplete, preventing parents from making informed decisions about whether to allow Facebook to collect their children’s sensitive personal information.

A. Facebook Messenger Kids does not have a COPPA-compliant mechanism for obtaining verifiable parental consent.

COPPA requires operators of online services directed at children to obtain verifiable parental consent before collecting, using, or disclosing sensitive information about children under 13.⁴ The consent mechanism must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child’s parent.⁵ Messenger Kids does not meet this requirement.

The Messenger Kids application allows anyone who has a Facebook account and claims to be an adult to create and “verify” an account for a child. The verification process works as follows: After the app is downloaded to a child’s device, someone (ostensibly the child’s parent) authenticates to the app with his or her Facebook username and password. That person can then create an account for the child and add contacts to the child’s contact list through the “parent’s” own Facebook account.⁶ The child is then able to send messages to the person who created the account and any of the child’s contacts.

This method is not “reasonably calculated, in light of available technology, to ensure that the person providing consent is the child’s parent.”⁷ The only prerequisites to creating a Messenger Kids account for a child are a Facebook account of a user who claims to be 18 or older and physical access to a child’s device. Because Facebook does not verify ages, the mere existence of a Facebook account is insufficient to establish that a person is an adult, much less that the supposed adult is a child’s parent or guardian.

The FTC has previously denied approval for a similar “verifiable parental consent” mechanism under COPPA.⁸ In 2013, the FTC rejected the application of AssertID, which proposed to use Facebook’s social graph as a method of authentication. AssertID’s product would have “ask[ed] a parent’s ‘friends’ on a social network to verify the identity of the parent and the existence of the parent-child relationship.” The method would have been “premised on verification by a

³ Facebook, *Messenger Kids Privacy Policy* (Dec. 4, 2017), <https://www.facebook.com/legal/messengerkids/privacypolicy>.

⁴ 15 U.S.C. § 6502(b)(1)(A)(ii).

⁵ 16 C.F.R. § 312.4.

⁶ Messenger Kids, <https://messengerkids.com/>.

⁷ 16 C.F.R. § 312.5(b)(1).

⁸ Under 16 C.F.R. § 312.12, companies may apply for the Commission’s approval of parental consent mechanisms not enumerated in Section 312.5(b).

minimum number of verifiers” and would have required “that a minimum ‘trust score’ be met” for approval.⁹

The Commission held that approval would be premature “without relevant research or marketplace evidence demonstrating the efficacy of social-graph verification and that such a method is reasonably calculated to ensure the person providing consent is the child’s parent.” The Commission was also “persuaded by commenters’ concerns about the reliability of social-graph verification.” It recognized that “users can easily fabricate Facebook profiles,” noted that about 8.7% of Facebook’s accounts at the time were fake, and cited comments “highlighting the fact that children under 13 have falsified their age information to establish social media accounts, including very active accounts with significant age-inflation.”¹⁰

Facebook’s parental consent mechanism for Messenger Kids is even less trustworthy than what AssertID proposed. Instead of relying on a person’s social graph, Facebook relies solely on a single user’s unverified assertions. As was the case with AssertID, Facebook has not shown any research or evidence that its verification method is reasonably calculated to ensure that the person providing consent is the child’s parent—or is even an adult.

Five years after the FTC rejected AssertID’s application, Facebook still cannot prevent fake accounts. Facebook reported last year that up to 270 million users were either “user-misclassified and undesirable” or duplicates of real accounts.¹¹ It is easy enough to create fake accounts that Russia used hundreds of them to interfere with the 2016 election.¹²

Our own testing shows that it is not difficult to create a fake account that can approve a Messenger Kids user. We created a brand new Facebook account for a fictional 18 year-old. We then used that account to approve a fictional Messenger Kids user. The entire process took five minutes.

What the FTC found in 2013 is still true: a Facebook account is insufficient to ensure that a person providing consent is the child’s parent.

⁹ Letter from Donald S. Clark, Secretary, FTC, to Keith Dennis, President, AssertID, Inc., FTC Matter No. P135415 (Nov. 12, 2013), <https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-denies-assertids-application-proposed-coppa-verifiable-parental-consent-method/131113assertid.pdf>.

¹⁰ *Id.*

¹¹ James Titcomb, *Facebook Admits up to 270m Users are Fake and Duplicate Accounts*, Telegraph (U.K.) (Nov. 2, 2017), <https://www.telegraph.co.uk/technology/2017/11/02/facebook-admits-270m-users-fake-duplicate-accounts/>

¹² Scott Shane, *The Fake Americans Russia Created to Influence the Election*, N.Y. Times (Sept. 7, 2017), <https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html>.

B. Facebook’s privacy policy for Messenger Kids is confusing and incomplete

The COPPA Rule also requires that notice to parents “must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory material.”¹³ Facebook’s notice fails this standard for two reasons. First, the notice is not clearly written or complete because it does not adequately inform parents about Facebook’s data-sharing practices. Second, the policy is incomplete because it does not clearly disclose how long Facebook retains children’s data.

Facebook’s privacy notice includes the following description of its third-party disclosure policy:

Our vendors and service providers. We may transfer information we collect to third party service providers that support our business, such as companies that provide technical infrastructure or support (like a content delivery network), provide customer service, or analyze how Messenger Kids is being used to help us improve the service. . . .

Facebook Family of Companies. Messenger Kids is part of Facebook, and we may share the information we collect in Messenger Kids within the family of companies that are part of Facebook to support the uses described above, and to improve the services provided by the FB family of companies. For example, parents use Facebook Messenger to communicate with their children on Messenger Kids, and Facebook uses information from Messenger Kids to support seamless cross-service communication.¹⁴

This language is vague and incomplete. It states that Facebook may transfer information to third parties to “support [its] business.” That phrase might be interpreted to cover almost anything, including transfers to advertising networks, data brokers, and analytics firms. Although Facebook lists non-exclusive examples of service providers that would support Facebook’s business, those examples could be interpreted narrowly or broadly. A parent reading that policy might reasonably assume a narrower interpretation of “support our business” while Facebook takes a broader view of the term. That ambiguity is confusing and potentially misleading.

The language in Facebook’s policy stating that data may be disclosed “to improve the services provided by the Facebook family of companies” is similarly vague.

¹³ 16 C.F.R. § 312.4(a).

¹⁴ Facebook, *Messenger Kids Privacy Policy* (Dec. 4, 2017), <https://www.facebook.com/legal/messengerkids/privacypolicy>.

Facebook’s reference to the “Facebook Family of Companies” is likewise confusing and incomplete. Facebook has acquired or merged with 66 different companies.¹⁵ Parents may not know which companies Facebook owns, and the Messenger Kids privacy policy does not say. Parents who want to know how widely Facebook might share their children’s data must find out for themselves by searching for a separate page that lists some, but not all, of the companies Facebook has bought. The Messenger Kids privacy policy does not even link to this page.

Facebook’s distinction between “the family of companies” and subsidiaries creates further confusion. According to Facebook’s “Help Center,” the “Facebook Family of Companies” includes Facebook Payments, the Onavo analytics company, WhatsApp, Oculus VR, Masquerade (whose products include face-tracking technologies), and the CrowdTangle social analytic platform.¹⁶ Missing from that list are “Facebook Products” such as Instagram, Messenger, Moments, Bonfire, Audience Network, and “other features, apps, technologies, software, products, or services.”¹⁷ Thus, even parents who manage to find the “Facebook Family of Companies” page would lack the information needed to give meaningful consent to the disclosure of their children’s sensitive personal information.

If Facebook does disclose information to third parties, its privacy notice may be incomplete by not naming them. Under the FTC’s COPPA Rule, a privacy notice must list “all operators collecting or maintaining personal information from children through the Web site or online service.”¹⁸ The FTC has long viewed “affiliates and subsidiaries” as third parties unless the affiliate relationship is clear to consumers.¹⁹ Thus, both third parties and companies owned by Facebook must be named.

Other required disclosures are also missing. For example, a privacy notice must tell parents that the operator “won’t require a child to disclose more information than is reasonably necessary to participate in an activity,” that parents “can agree to the collection and use of their child’s information, but still not allow disclosure to third parties unless that’s part of the service,” and

¹⁵ Steve Toth, *66 Facebook Acquisitions – The Complete List (2018)*, TechWyse (Jan. 24, 2018), <https://www.techwyse.com/blog/infographics/facebook-acquisitions-the-complete-list-infographic/>.

¹⁶ Facebook, *The Facebook Companies*, <https://www.facebook.com/help/111814505650678> (last visited Sept. 15, 2018).

¹⁷ Facebook, *What are the Facebook Products?*, <https://www.facebook.com/help/1561485474074139> (last visited Sept. 15, 2018).

¹⁸ 16 C.F.R. § 312.4(d)(1).

¹⁹ *Protecting Consumer Privacy in an Era of Rapid Change* 42, FTC (Mar. 2012), <http://ftc.gov/os/2012/03/120326privacyreport.pdf> (“The Commission maintains the view that affiliates are third parties, and a consumer choice mechanism is necessary unless the affiliate relationship is clear to consumers”).

that parents have the right to direct the operator to delete their child’s personal information.²⁰ These disclosures are either missing or incomplete in the Messenger Kids privacy notice.

The disclosures regarding parents’ rights to have their children’s personal information deleted are especially confusing and incomplete. The COPPA Rule requires that “an operator shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected.”²¹ But the Messenger Kids privacy notice does not clearly indicate that Facebook deletes personal information on children when it is no longer needed.

Every message a child sends with Messenger Kids is “personal information.” Personal information protected by COPPA includes “information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in [15 U.S.C. § 6501(8)].”²² A message from a child necessarily contains some “information concerning the child.” Each message on Messenger Kids is associated with the name of the child who sent or received the message. Thus, messages sent or received on Messenger Kids are personal information that Facebook must delete at a parent’s direction.

Facebook’s policy does not comply with that requirement. According to the Messenger Kids privacy notice, parents who want to stop Facebook from collecting their child’s personal information must delete their child’s account, at which time Facebook “will delete [the child’s] Messenger Kids registration information, information about their activity and contacts, and device information.”²³ The privacy notice does not state how long Facebook retains this information if a parent has not deleted his or her child’s account. The privacy notice also tells parents that “the messages and content your child sent to and received from others before their account was deleted may remain visible to those users.”²⁴ It is unclear how long those messages, which must remain on Facebook’s servers to be visible to any users, will stay visible.

C. Conclusion

Messenger Kids poses developmental risks for children. It also violates COPPA. Facebook does not obtain verifiable parental consent via a mechanism reasonably calculated to ensure that the person giving consent is the child’s parent, or even an adult. And Facebook does not give parents sufficient notice of its data practices to allow parents to make an informed choice whether to allow Facebook to access children’s personal information. We ask the Commission

²⁰ FTC, *Children’s Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business* (June, 2017), <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>. See also 16 C.F.R. § 312.4(d).

²¹ 16 C.F.R. § 312.10.

²² 15 U.S.C. § 6501(8)(G).

²³ Facebook, *Messenger Kids Privacy Policy* (Dec. 4, 2017), <https://www.facebook.com/legal/messengerkids/privacypolicy>.

²⁴ *Id.*

to investigate Facebook’s violations of COPPA and to take all enforcement actions necessary to ensure compliance with the law.

Respectfully Submitted,

James T. Graves*
Angela J. Campbell
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Ave NW, Suite 312
Washington, DC 20001
James.Graves@law.georgetown.edu
202-662-9545
*Counsel for Campaign for a Commercial-Free
Childhood*

Campaign for a Commercial-Free Childhood	Parents Across America
Badass Teachers Association	Parents Television Council
Centre for Child Honouring	Peace Educators Allied for Children Everywhere (P.E.A.C.E.)
Consumer Federation of America	Public Citizen
Defending the Early Years	The Story of Stuff
Electronic Privacy Information Center	TRUCE (Teachers Resisting Unhealthy Childhood Entertainment)
Media Education Foundation	United Opt Out National
MomsRising/MamásConPoder	USPIRG
New Dream	
Parent Coalition for Student Privacy	

* This letter was drafted primarily by Jae Ahn, a law student in the Institute for Public Representation Communication & Technology Clinic, under the supervision of clinic attorneys.