PAUL HASTINGS

STAY CURRENT

June 2017

Follow @Paul_Hastings

Complying with COPPA: FTC Releases Updated Six-Step Compliance Plan for Businesses

By Behnam Dayanim & Mary-Elizabeth M. Hadley

Earlier this week, the Federal Trade Commission ("FTC" or the "Commission") issued an updated Six-Step Compliance Plan for Businesses ("Updated Plan") to comply with the Children's Online Privacy Protection Act ("COPPA") Rule.[1] The Updated Plan provides businesses with guidance on how to know whether they are subject to COPPA—a law designed to protect children under age 13 as they access the internet—and on how to comply with the Rule's requirements if so.

This alert summarizes the two key changes in the Updated Plan. Additionally, we provide a short refresher on the six steps your company should take when considering COPPA.

I. Two Key Changes

1. **New Companies Covered.** The Updated Plan makes clear that companies providing "connected toys or other Internet of Things [IoT] devices" are covered by COPPA. As more companies enter the IoT space, including by offering products designed for children that collect voice recordings, geolocation data and other personal information, it will be important for them to assess their obligations under COPPA.

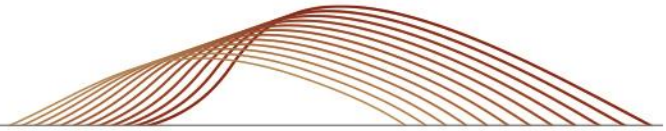
2. **Two New Ways to Obtain Parental Consent.** Obtaining parents' permission prior to collecting information online from children under 13 is one of the most important—and most challenging—elements of COPPA. The Updated Plan includes two new recently-approved methods for obtaining parental consent: (a) asking knowledge-based authentication questions, and (b) utilizing facial recognition technology to compare a picture of a driver's license or other photo ID submitted by the parent against a second photo from the parent.

II. Six-Step Compliance Plan:

1. Step One – Determine Whether COPPA Applies to Your Company

As a threshold matter, recognize that COPPA only applies to operators of websites and online services that collect personal information of children under the age of 13. More specifically, compliance with COPPA is required if:

[1] The FTC enforces COPPA through the COPPA Rule, which specifies what operators of websites and online services must do to protect children's online privacy and safety.



- Your website or online service is **directed to children under 13**, and you (a) **collect** their personal information; or (b) **permit others to collect** those children's personal information; or

- Your website or online service is directed to a **general audience**, but you have **actual knowledge** that you collect personal information from children under 13; or

- You provide an **advertising network or plug-in**, for example, and you have **actual knowledge** that you collect personal information from users of a website or service directed to children under 13.

To help companies further understand whether they are subject to COPPA, the FTC provides guidance on a number of key terms:

- "**Website or online service**" – COPPA broadly defines this term in a way that includes not only traditional websites, but also (i) **mobile apps** that send or receive information online (including network-connected games, social networking apps and apps delivering behaviorally-targeted ads); (ii) **internet-enabled gaming platforms**; (iii) **plug-ins**; (iv) **ad networks**; (v) internet-enabled **location-based services**; and the newly-enumerated (vi) **connected toys or other IoT devices**.

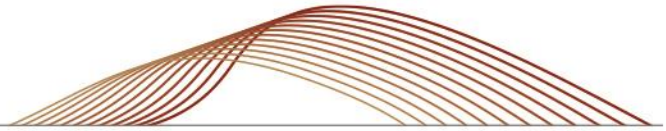
- "**Directed to children under 13**" – The Commission considers numerous factors to determine whether a site or service is directed to children under age 13, including: (i) its **subject matter**; (ii) **visual and audio content**; (iii) references to **child celebrities** or celebrities who appeal to children; (iv) the presence of **child-directed ads**; and, more generally, (v) **other reliable evidence** about the age of the actual or intended audience.

- **"Personal Information"** – In addition to traditional data elements such as **name**, home or other physical **address**, **telephone number** and **Social Security number**, the FTC makes clear that personal information under COPPA also includes **online contact information** (e.g., an email address or other identifier that permits someone to contact a person directly, including an IM, VoIP or video chat identifier); a **persistent identifier that can be used to recognize a user over time and across different sites** (e.g., a cookie number, an IP address, a processor or device serial number or a unique device identifier); **a photo, video or audio file containing a child's image or voice**; **geolocation information** sufficient to identify a street name, city or town; and **other information** about the child or parent that is collected from the child and **combined with one of these identifiers**.

2. Step Two – Post a COPPA-Compliant Privacy Policy

For those subject to COPPA, the next step is to **post a privacy policy that clearly and comprehensively describes how you collect, use and share information** collected online from children under 13. This policy must describe not only your own information collection practices, but also those of plug-ins, ad networks or any others collecting personal information on your site or service.

Additionally, be sure to inform parents about their rights, including (i) that you will not require a child to disclose more information than is reasonably necessary to participate in an activity; (ii) that they can review their children's personal information, direct you to delete it and refuse to permit any further collection or use of their child's information; (iii) that, unless disclosure is part of the service



(e.g., social networking), they can agree to collection and use—but not disclosure to third parties—of their child's personal information; and (iv) the procedures to exercise their rights.

Links to your privacy policy should be clearly and prominently provided on your homepage and anywhere you collect personal information from children. If you operate a general audience site or service, but have a separate children-directed section, post a link to your privacy policy on the homepage of the children's part of the site or service.

3. Step Three – Provide Parents with Direct Notice Before You Collect their Children's Information

Companies subject to COPPA must also provide parents "direct notice" of their information practices prior to collecting children's information. Additionally, should the company materially change its practices, an updated direct notice is required.

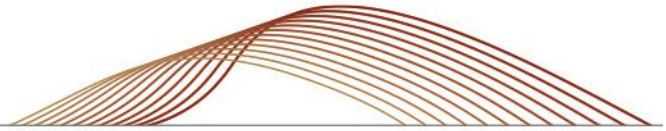
The parental notice—which must be clear and easy to read—must inform parents:

- that you **collected their online contact information** for the **purpose of getting their consent**;
- that you **want to collect personal information from their child**;
- that their **consent is required for the collection, use and disclosure** of the information;
- the **specific personal information you want** to collect and **how it might be disclosed** to others;
- a **link** to your online privacy policy;
- **how to consent**; and
- that if the parent **does not provide consent within a reasonable time**, you **will delete** the **parent's online contact information** from your records.

4. Step Four – Obtain Parents' Verifiable Consent Before Collecting their Children's Information

Next, prior to collecting, using, or disclosing a child's personal information, companies must obtain **verifiable consent** from their parent. The FTC seeks to provide some flexibility to consider new methods, charging operators with selecting a method reasonably designed in light of available technology to ensure that the person giving the consent is the child's parent. Acceptable methods approved to date include:

- **Print & Send.** Providing a consent form for the parent to sign and return via mail, fax or scan;
- **Credit/Debit Card.** Requiring the parent, in connection with a monetary transaction, to use a credit or debit card or other online payment system that provides the primary account holder with notifications of each discrete transaction;



- **Telephone or Videoconference.** Asking the parent to call a toll-free phone number staffed by trained personnel, or connect to trained personnel via videoconference;

- **Email Plus.** Emailing the parent and having them respond via return email, provided you (a) take an additional confirmatory step (the "plus") such as requesting that the parent provide a phone number or mailing address so that you can follow up or, after a reasonable time, sending another message to confirm consent; and (b) will not be disclosing the personal information to third parties or making it publicly available.

- **Knowledge-Based Challenge Questions (New).** Asking the parent to answer a series of knowledge-based challenge questions that would be difficult for someone other than him or her to answer; and

- **Facial Recognition-Facilitated Photo Matching (New).** Verifying a picture of a driver's license of other photo ID submitted by the parent and then comparing that photo to a second photo submitted by the parent.

5. Step Five – Honor Parent's Ongoing Rights Regarding their Children's Information

Once you have the parent's consent, you will still need to recognize that parents have ongoing rights related to their children's information. If a parent asks you to do so, you must: (i) **enable them to review** the personal information you have collected from their child; (ii) provide them a way to **revoke their consent** and prohibit further processing of personal information from their child; and (iii) **delete** their child's personal information.

6. Step Six – Take Reasonable Measures to Protect the Security of Children's Information

Finally, the FTC reminds companies that COPPA requires them to establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children. Basic principles include:

- **Data Minimization.** Minimizing what you collect initially;

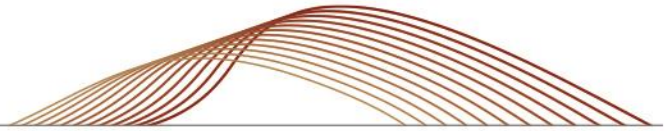
- **Third-Party Management.** Taking reasonable steps to share personal information only with service providers and third parties that are capable of maintaining its confidentiality, security and integrity, and obtaining assurances from the vendors they will fulfill such obligations;

- **Data Retention.** Retaining personal information collected from children only for as long as reasonably necessary for the purposes for which it was collected; and

- **Disposal.** Securely disposing of information once you no longer have a legitimate reason to retain it.

Of course, these are sound practices which we recommend to all companies, not just those processing personal information of children, and we are happy to help implement them.

✧ ✧ ✧



If you have any questions concerning these developing issues, please do not hesitate to contact any of the members of our Privacy and Cybersecurity Practice, including these Paul Hastings lawyers:

Washington, D.C.

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Robert P. Silvers
1.202.551.1216
robertsilvers@paulhastings.com

Sherrese M. Smith
1.202.551.1965
sherresesmith@paulhastings.com

Mary-Elizabeth M. Hadley
1.202.551.1750
maryelizabethhadley@paulhastings.com

San Francisco

Thomas P. Brown
1.415.856.7248
tombrown@paulhastings.com

Thomas A. Counts
1.415.856.7077
tomcounts@paulhastings.com

Paul M. Schwartz
1.415.856.7090
paulschwartz@paulhastings.com