

Richard B. Newman Attorney  
 newman@hinchnewman.com  
 Hinch Newman LLP, New York

# Complying with the FTC's COPPA rule in a data-driven world

The US Federal Trade Commission ('FTC') enforces the Children's Online Privacy Protection Act of 1998 ('COPPA'), which sets forth what operators of websites and apps must do to protect the online privacy and safety of children under 13 years of age. Richard B. Newman, Attorney at Hinch Newman LLP, provides a breakdown of the requirements under COPPA and what entities must know in order to lawfully collect the personal information of children.

The FTC's Division of Privacy and Identity Protection has been extremely active of late investigating and taking action against those that compromise the online privacy of children by failing to obtain parental consent before collecting their personal information. In fact, the FTC has brought more than 20 COPPA cases and collected millions of dollars in civil penalties. Of particular interest to the FTC are internet-connected or smart toys and other devices directed at children. COPPA is also vigorously enforced by state attorneys general.

## Who must comply with COPPA?

Simply stated, COPPA applies to operators of websites and online services that collect personal information from children under 13. You must comply with COPPA if:

- your website or online service is directed to children under 13 and you collect their personal information;
- your website or online service is directed to children under 13 and you let others collect their personal information;
- 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

- your company runs 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.

## The broad definition of 'website or online service'

COPPA defines 'website or online service' broadly. In addition to standard websites, examples of others covered by COPPA include mobile apps that send or receive information online, such as network-connected games, social networking apps or apps that deliver behaviourally-targeted ads; internet-enabled gaming platforms; internet-enabled location-based services; Voice-over Internet Protocol ('VoIP') services; and connected toys or other Internet of Things devices.

## 'Directed to children under 13'

The FTC looks at a variety of factors to determine if a website or service is directed to children under 13, including the subject matter of the website or

service, visual and audio content, 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 children, advertisements that are directed to children, and other reliable evidence about the age of the actual or intended audience.

If a website does not target children as its primary audience, but is 'directed to children under 13,' the operator may choose to apply COPPA protections only to users under 13. In such cases, operators are proscribed from collecting personal information from users without first collecting age information. Moreover, the FTC makes clear that operators must not collect any personal information from users that say they are under 13 until verifiable parental consent has been obtained.

## Definition of 'personal information' and 'collect'

Under COPPA, personal information includes:

- full name;
- home or other physical address,

## If another company collects personal information through a child-directed site or service, such as through an advertising network or plug-in, the operator is responsible for complying with COPPA.

- including street name and city or town;
- online contact information like an email address or other identifier that permits someone to be contacted directly;
- screen name or user name where it functions as online contact information;
- telephone number;
- social security number;
- a persistent identifier that can be used to recognise a user over time and across different sites, including a cookie number, an IP address, a processor or device serial number, or a unique device identifier;
- a photo, video, or audio file;
- sufficient geolocation information to identify a street name and city or town; and
- other information about the child or parent that is collected from the child and is combined with one of these identifiers.

Under COPPA, collection includes requesting, prompting or encouraging the submission of information, even if it is optional; letting information be made publicly available (for example with an open chat or posting function) unless the operator takes reasonable measures to delete all or virtually all personal information before postings are public and deletes all information from its records; or passively tracking a child online.

If another company collects personal information through a child-directed site or service, such as through an advertising network or plug-in, the operator is responsible for complying with COPPA. If the operator possesses actual knowledge that it is collecting personal information directly from users of a child-directed site or service, the operator is also responsible for complying with COPPA.

### Privacy policies

If covered by COPPA, operators must post a clear and conspicuous privacy policy that thoroughly describes how personal information collected online from children under 13 is handled. The privacy policy must describe both the operator's practices and the practices of any others collecting personal information on the website or service.

A link to the privacy policy should be posted on the homepage and anywhere personal information is collected from children. General audience websites or services that possess a separate section for children should include a link to the privacy policy on the homepage of the children-designated portion thereof.

Links to privacy notices should be prominent, in a larger font or different colour type on a contrasting background. A mouseprint link at the bottom of the page – below the fold – that is not distinguishable from other links will not suffice.

The FTC recommends that privacy policies be simple to read and include, without limitation, a list of all operators collecting personal information, along with names and contact information; a description of the personal information collected, and how it is collected and used; and a description of parental rights and the procedures to follow to exercise their rights.

**Providing parents with direct notice of information practices**  
COPPA requires that operators provide parents with 'direct notice' of information practices before collecting information from their children. In addition, material changes to previously agreed to practices require updated notices.

The notices must include, without limitation, that online contact information has been collected for the purpose of getting their consent; that the operator wants 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 the operator wants to collect and how it might be disclosed; a link to the online privacy policy; how the parent can provide consent; and that if the parent does not consent within a reasonable time, the operator will delete their online contact information from its records.

In certain circumstances, it may be acceptable to collect a narrow class of personal information without

obtaining parental consent. However, parents must still be provided with direct notice of the activities.

**The requirement of 'verifiable consent'**  
Prior to collecting, using or disclosing personal information from a child, verifiable parental consent is required. This is a key component of COPPA.

According to FTC guidance, the method chosen must be reasonably designed in light of available technology to ensure that the person providing the consent is the child's parent. If the operator has actual knowledge that it is collecting personal information from a website or service that is directed to children, it may obtain consent directly or through the child-directed website or service.

The FTC has stated that acceptable methods include having the parent sign a consent form and send it back via fax, mail or electronic scan; using a credit card, debit card or other online payment system that provides notification of each separate transaction to the account holder; calling a toll-free number staffed by trained personnel; connecting to trained personnel via video conference; providing a copy of a form of government-issued ID that is checked against a database, as long as it is deleted when the verification process is completed; answering a series of knowledge-based challenge questions that would be difficult for someone other than the parent to answer; or verifying a picture of a driver's licence or other photo ID submitted by the parent and then comparing that photo to a second submitted photo using facial recognition technology.

If a child's personal information will only be used for internal purposes and will not be disclosed, the operator may use a method known as 'email plus.' An email is sent to the parent with a request to respond with consent. The operator must send a confirmation to the parent via email, letter or telephone call. The parent must also be advised that they can revoke consent at any time. Moreover, the parent must be provided with the option of allowing the collection and use of their child's personal information

If covered by COPPA, operators must post a clear and conspicuous privacy policy that thoroughly describes how personal information collected online from children under 13 is handled. The privacy policy must describe both the operator's practices and the practices of any others collecting personal information on the website or service.

continued

without agreeing to the disclosure of that information to third parties.

#### Parents' ongoing rights

Even if parents have agreed to the collection of their child's information, they have ongoing rights and operators have continuing obligations.

If a parent asks for it, the operator must provide a way to review the personal information collected from their child; a way to revoke consent and refuse the further use or collection of personal information; and must delete the personal information.

Importantly, any time an operator communicates with a parent about personal information already collected from their child, reasonable steps must be taken to ensure that the operator is, in fact, dealing with the child's parent. Additionally, methods utilised to provide parents access to information collected from their children cannot be unduly burdensome on the parent.

#### Reasonable procedures to protect personal information

COPPA requires that reasonable procedures to protect the confidentiality, security and integrity of personal information be established and maintained. Operators should minimise what is collected and personal information should only be released to service providers and third parties capable of maintaining its confidentiality, security and integrity. In addition, operators should obtain written assurances that such third parties will live up to those responsibilities, and personal information should be retained only as long as is reasonably necessary for the purpose for which it was collected, and should be disposed of once there no longer exists a legitimate reason for its retention.

#### COPPA's application to voice recordings

The FTC recently provided additional guidance on how COPPA applies to the collection of audio voice recordings. In an October 2017 policy enforcement statement, the FTC noted that the COPPA rule requires websites and online services directed at children to obtain verifiable parental consent before collecting an audio recording. In doing so, the FTC expressed its recognition of the value of using voice as a replacement for written words in performing search and other functions on internet-connected devices.

The FTC stated that it will not initiate an enforcement action against an operator for not obtaining parental consent before collecting an audio file with a child's voice when it is collected solely as a replacement of written words, such as to perform a search or to fulfil a verbal instruction or request, as long as it is held for a brief time and only for that purpose.

There are, of course, important limitations to this policy. It does not apply when the operator requests information via voice that would otherwise be considered personal information, such as a name. In addition, an operator must still provide clear notice of its collection and use of audio files and its deletion policy in its privacy policy.

Also, the operator may not make any other use of the audio file before it is destroyed and the policy does not affect the operator's COPPA compliance requirements in any other respect.

#### Noteworthy COPPA enforcement actions and trends

In 2016, a Singapore-based mobile advertising company paid \$950,000 in civil penalties and was required to implement a comprehensive privacy programme to settle FTC

charges that it deceptively tracked the locations of hundreds of millions of consumers, including children, without their knowledge or consent, to serve them geo-targeted advertising. The FTC alleged that the company misrepresented that its advertising software would only track consumers' locations when they opted-in and in a manner consistent with their device's privacy settings. According to the FTC, the company was tracking consumers' locations regardless of whether the apps using the software asked for their permission to do so, and even when consumers had denied permission to access their location information.

The FTC also recently reached a settlement with two app developers that allowed third-party advertisers to collect information about children without parental consent. The developers paid a combined \$360,000 in civil penalties for alleged COPPA violations. This settlement is noteworthy because it was the first in which the FTC alleged that companies allowed advertisers to use persistent identifiers – pieces of data that are tied to a particular user or device – to advertise to children. Persistent identifiers were among the categories added to COPPA's definition of personal information when it was updated in 2013.

Child advocacy and privacy groups have recently called on the FTC to investigate several smartwatch brands and the privacy risks they pose to children. The advocacy groups, including the Electronic Privacy Information Center, the Center for Digital Democracy and the Consumer Federation of America, claim that some of the popular smartwatch models are hackable. The FTC has clearly evidenced a willingness to aggressively scrutinise compliance with COPPA and data security issues related to the Internet of Things.