TOY INDUSTRY CHECKLIST FOR MOBILE APPS AND PROMOTIONS

Second Edition | May 2014

Toy Industry Association, Inc.

FOREWORD

Members of the toy industry are fast embracing the world of mobile applications ("apps").

Apps offer a new world of engaging content alongside new branding and marketing opportunities. However, regulators and legislators are examining app privacy and data security, and plaintiff's attorneys are targeting app providers and platforms for privacy and security lapses. Mobile apps can be directed to kids, triggering children's privacy compliance obligations. The app landscape is complicated further because toy companies can be involved in the app "ecosystem" through a variety of ways. They may develop company-branded apps directly or with a developer. They may license properties to app developers. They may advertise via in-app advertisements, working through advertising agencies or other third parties, and thus have no direct contact with the app developer or provider.

The Toy Industry Association (TIA) has developed this *Checklist for Mobile Apps and Promotions* as a framework that both member and non-member companies can use to examine and evaluate the risks and opportunities related to app initiatives. Because of the complexity of apps, and the varying level of knowledge and awareness of legal implications of app initiatives within the industry, this *Checklist* provides detailed information to help all toy industry stakeholders engage in a robust review of the app initiative or app development process.

While this *Checklist* does not constitute legal advice, and TIA recommends that members consult with experts on their specific app questions, it is designed to help members identify issues and possible solutions to protect the company's legal and reputational interests in its app-related activities.

TOY INDUSTRY CHECKLIST FOR MOBILE APPS AND PROMOTIONS
Second Edition | May 2014

Prepared for the Toy Industry Association by
KELLER AND HECKMAN LLP
1001 G Street N.W. | Washington, D.C. 2000

Approved by
TIA Responsible Marketing to Children Committee

TABLE OF CONTENTS

Questions and comments on this guidance document can be directed to info@toyassociation.org

OVERVIEW

This *TOY INDUSTRY CHECKLIST FOR MOBILE APPS AND PROMOTIONS* is based on current thinking in an area that is rapidly changing in a manner that may alter the landscape and affect best practices. As a result of many recent developments and evolving concerns about mobile apps, toy industry members should keep these important principles in mind:

1) Understand what data is collected through an app, offer a privacy policy, adhere to children's privacy requirements in kid-directed apps, and make sure that data is appropriately protected from disclosure, alteration or breach.
2) Apps that are not free should clearly state their cost. Those advertised as "free" should not contain hidden or misleading costs.
3) Apps should not directly suggest or ask children to buy products or attempt to persuade children to ask adults to do so.
4) Payment arrangements should be clear to consumers and purchases should not be made through default settings without consumers' explicit consent.
5) App makers should provide contact information that clearly identifies them to allow consumers to ask questions or submit concerns or complaints.

Here are just some of the significant recent developments relevant to these general recommendations:

- On December 19, 2012, the Federal Trade Commission ("FTC") issued final amendments to the Children's Online Privacy Protection Rule ("COPPA Rule"). The new rules took effect on July 1, 2013. Mobile apps directed to children are now expressly subject to COPPA. Significantly, the FTC revised the definition of "personal information" to include persistent identifiers, such as an Internet Protocol (IP) address, a customer number held in a cookie, or a unique device identifier (UDID). If used in support of internal operations, but not for tracking or behavioral advertising, collection of persistent identifiers is acceptable. On the other hand, "personal information" now also includes precise geolocation information as well as photos, videos and audio files, even when this information is not connected to contact information, like an e-mail address. Collection of this information at child-directed websites, online services or apps requires verifiable parental consent.

- The FTC and state Attorneys General have the ability to initiate enforcement actions under COPPA. The FTC initiated at least one enforcement action for COPPA violations related to an app even before the rule was updated. In 2011, in its first case involving mobile apps, the FTC entered into a consent order with W3 Innovations LLC, the developer of child-directed mobile apps, for alleged violations of COPPA and the COPPA Rule, pursuant to which the company agreed to pay $50,000. The FTC alleged that the company illegally collected and disclosed e-mail addresses from tens of thousands of children under the age of 13 without their parents' prior consent and allowed children to publicly post information, including personal information, on message boards. In November 2013, the New Jersey Attorney General's office announced that it settled alleged COPPA violations by an app developer, Dokogeo, Inc. The Attorney General alleged that the company's Dokobots app and associated website were directed to children and violated COPPA, the amended COPPA Rule, and New Jersey's Consumer Fraud Act by failing to age-screen visitors and obtain verifiable parental consent. In December 2013, the Center for Digital Democracy ("CDD") filed a complaint with the FTC alleging that a Hello Kitty mobile app operated by Sanrio Digital violated the notice and consent requirements under COPPA; it also asserted in a separate complaint that a Marvel comics website engaged in COPPA violations. CDD subsequently filed a second complaint that Marvel's updated privacy policy did not comply with COPPA.

- The National Telecommunications and Information Administration ("NTIA") released a self-regulatory *Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices* in July 2013 pursuant to the White House's framework, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. The purpose of the voluntary Code is to provide consumers with transparency about how mobile app providers collect and share personal data. While the Code represents a useful discussion, it comes with no obligation to adopt it, and apps directed to children must comply with the requirements of COPPA. There is no official guidance from the FTC suggesting that the icons and short form notices in the NTIA framework will meet all applicable notice obligations under COPPA.

- The FTC held a public workshop on mobile payments, as well as a workshop to discuss privacy and other disclosures in the online and mobile media. These initiatives led to revisions to the FTC's Dot Com Disclosures guide in May, 2013. This guide provides further information on the FTC staff's interpretation of how principles of federal advertising law apply to online and mobile advertising and sales.

- In January 2014, the FTC reached an agreement with Apple Inc. pursuant to which the company will refund at least $32.5 million to consumers to settle complaints that the company billed consumers for millions of dollars of charges incurred by children in kids' mobile apps.[1] The settlement is very significant, in part because the FTC deemed the billing "unfair" under Section 5 of the FTC Act. Most FTC enforcement action occurs under the "deception" prong of Section 5.

- Google was recently named in a class action lawsuit about allegedly unauthorized in-app purchases by children using Android devices. The complaint alleges that games are deliberately "addictive" and "compel" children to purchase in-game currency to continue to play.[2] Similar to the allegations the FTC leveled against Apple, the complaint asserts that once a Google user inserts a password, purchases can be made for up to 30 minutes without reentering the password or obtaining authorization from a parent. Plaintiffs point to the fact that Google applies its own rules to apps, and reviews and approves them before posting, as a basis to hold Google responsible for the in-app activities. It also cites standard contract law for the principle that contracts entered into by minors may be disaffirmed.

- In the wake of a privacy consent agreement with major app platforms, the California Attorney General's Privacy Enforcement and Protection Unit released guidance for mobile apps, *Privacy on the Go: Recommendations for the Mobile Ecosystem*, in January 2013.

- Legislation has been proposed that will affect privacy in general and mobile app privacy in particular. Self-regulatory developments continue through organizations like the Mobile Marketing Association (MMA), The Wireless Association (CTIA), the Digital Advertising Alliance (DAA), and the Network Advertising Initiative (NAI). A self-regulatory program for online behavioral advertising (OBA) has been in place for websites for several years, and last year DAA and NAI each released guidance relating to OBA on mobile devices.

- Outside the U.S., the United Kingdom's now-defunct Office of Fair Trading issued *Principles for Online and App-Based Games*.[3] The document followed an investigation into the ways that online and app-based games encourage children to make purchases. The document offers one example of a European Union member state's analysis of situations that constitute good or bad practices within the EU.

Most privacy issues related to app use come from app developers inserting third party codes or software development kits (SDKs) into the app. Some of the most talked about app privacy lapses involve instances where

[1] FTC, *Apple Inc. Will Provide Full Consumer Refunds of At Least $32.5 Million to Settle FTC Complaint It Charged for Kids' In-App Purchases Without Parental Consent* (Jan. 15, 2014), www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million.

[2] *Imber-Gluck et al v. Google*; Case No. 5:14 CV-01070-PSG, filed March 7, 2014 (N.D. Cal.), s3.amazonaws.com/s3.documentcloud.org/documents/1070126/class-action-against-google-over-in-app-purchases.pdf.

[3] OFT, *Principles for online and app-based games* (Feb. 2014), www.oft.gov.uk/shared_oft/consumer-enforcement/oft1519.pdf.

codes allow the developer or platform to access the consumer's contact list, alter default settings, or identify their precise location. If this type of information is collected by or transmitted to a toy company via a kid-directed app, it will violate COPPA. Even where the app is directed to adults, if the consumer is not advised and offered a choice about the practice, regulatory investigations and litigation claiming the practice is unfair and privacy-invasive may well follow. Protecting the member company against such charges starts with mapping the data. This is basically an audit of what information is collected, such as personal contact details (like name, e-mail address, mobile phone number, etc.); device identifiers like IP addresses or UDIDs; geolocation information; passwords; photos; and "tracking" data. Because notions of how to define "personally identifiable information" (PII) are evolving, it is important that the audit identifies *all* data collected, whether it is combined with other data, and whether it is appended to or combined with data from third parties. It is also important to identify how the information will be used.

The prospect of both federal and state enforcement actions and other legal challenges underscores the need for app developers to document the intended target audience, make business decisions about whether age-screening should be built into the app, assure that they offer a well-designed and clear privacy policy, and consider the implications of in-app advertising, purchases and other app activities.

Basic questions to ask include:

1) Who is the intended audience?
2) What information is collected?
3) Is it necessary to collect the information to offer the app or related services?
4) Are information collection practices consistent with consumer expectations of privacy?
5) Are other activities and options, like purchase opportunities, clear and fair to the intended consumer?

Other legal issues that should be considered by toy companies include intellectual property protections; contractual considerations, including warranties and indemnifications; and availability of risk-shifting devices, like insurance. Toy companies should adopt contractual instruments to obtain assurances and indemnifications from its business partners regarding compliance with privacy and data security laws and best practices, IP ownership and clearances and the like.

Regardless of whether a toy company develops its own branded app using a third party or offers advertising, marketing or promotional opportunities through in-app advertisements, companies should seek to have a fundamental understanding of information collection capabilities of the app.

The goal is to affirm that the app:

1) meets applicable legal standards (such as COPPA);
2) is consistent with the member company's brand values;
3) will meet consumer expectations and business commitments regarding privacy; and
4) avoids claims or practices that might be considered false, misleading, deceptive or unfair.

Thinking about privacy and data security at the outset – requiring that apps incorporate privacy by design – will assure that information collection is transparent and appropriate choices are offered. Working through this checklist will help toy companies do that. From a technical perspective, this means that in developing an app, the checklist should be applied *at the latest* during the alpha or beta stage of the development process. This will minimize legal risk and help toy companies build their brands by offering fun, engaging apps that reflect privacy and data security best practices.

TOY INDUSTRY CHECKLIST FOR MOBILE APPS AND PROMOTIONS

This privacy and data security checklist applies to a toy company's participation in both in-app advertising and promotional initiatives and the development of company-branded mobile apps. Regardless of who develops the app, ideally the toy company should understand what information, if any, is collected via the app, how that information is stored, whether it is combined with other data, and with whom it is shared.

General Privacy and Data Security Considerations

It is essential to identify whether any personal or non-personal information is collected via the app either directly by the toy company or indirectly by the app developer or provider to be shared with the toy company.

The best rule of thumb: only the information needed to offer the app should be collected. Consent is advisable for certain types of information collection. For in-app advertisements, the burden is on the third-party agency to confirm the information collected and opt-in choices for geolocation. The toy company should closely scrutinize any app that permits or requires the collection of geolocation data and make sure that the app does not circumvent users' default settings on their browser. Offering clear choices to consumers is key to avoiding adverse PR and potential liability exposure for alleged privacy violations.

☐ **Does the app collect any personally identifiable information?** ☐ **Yes** ☐ **No**

If YES … require the app developer to complete a privacy audit checklist or review the app privacy policy to determine:

- What personal information is collected via the app (*e.g.,* name, address, e-mail, telephone number, etc.).
- Is a user name and password necessary.
- What, if any, geolocation information is collected via the app (*e.g.*, tagging to check in on social networking sites, send coupons based on mobile location, etc.).
- What, if any, non-personal information is collected via the app (*e.g.,* unique device identifier, pixel tags, cookies, etc.).
- Whether any sensitive data, like financial, health or children's data, is collected via the app.

  Note: COPPA rules apply to the collection of information from children, and appropriate security will be needed if children's or other sensitive data is collected.
- Who collects the information (toy company, the app developer, app platform provider, or other third party).

  Note: This determines who the "operator" of the app may be for purposes of laws such as COPPA.
- With whom any information is shared or disclosed.
- Where this information is stored.
- Whether this information is combined with any other information.
- How this information is protected (e.g., stored encrypted, anti-virus software, firewalls, etc.)

☐ **Does the app collect any geolocation information?** ☐ **Yes** ☐ **No**

If YES …

– Does the app require explicit opt-in consent from the user before collecting the geolocation data (*e.g.,* is there an "Allow/Disallow" option prior to the information being collected)? ☐ Yes ☐ No

– Does the app have a periodic schedule to renew opt-in consent? ☐ Yes ☐ No

If so, what is the schedule?

– Does the app collect geolocation data at all times? ☐ Yes ☐ No

-or-

– Does the app collect geolocation data only when the app is in use? ☐ Yes ☐ No

– Is collection of geolocation information essential to app functionality? ☐ Yes ☐ No

☐ **Does the app access the consumer's contact list?** ☐ **Yes** ☐ **No**

If YES …

– Does this occur because there is a functional need to do this in order for the app to achieve its purpose (*e.g.,* social networking) and only after the user has given express consent? ☐ Yes ☐ No

Note: Absent a functional reason to access contact information, ask if such an initiative reflects your company's consumer values even with consent.

☐ **Is any data collected by the app collected directly by the toy company or by an agent on its behalf?** ☐ **Yes** ☐ **No**

If YES …

– You are responsible for advising the consumer about privacy practices, in whole or in part.

☐ **Is any of the data that is collected via the app shared with third parties (including the toy company) or do third parties use technology to track the app user?** ☐ **Yes** ☐ **No**

If YES ...

– Is the sharing of the data expected and consistent with the app's use (*e.g.*, sharing with a fulfillment house to fulfill a mobile purchase made via an app)? ☐ Yes ☐ No

– Is app analytical data collected to develop audience metrics? ☐ Yes ☐ No

Note: If yes, and the app is directed to children under 13, this should nevertheless constitute support for the internal operations of the app.

– Is analytical data collected for purposes such as behavioral advertising or other similar purposes? ☐ Yes ☐ No

Note: If yes, and the app is directed to children under 13, this will violate COPPA

If NO …

- Is express consent from the user obtained if sharing falls outside of reasonable expectations or what is necessary to fulfill a request? ☐ Yes ☐ No

  Note: Some unexpected uses may include the following:

  - Sharing data with an advertising network for behavioral or targeted advertising.
  - Working with third parties to allow other transactional data to be appended and used across sites.
  - Accessing contact information contained in the user's address book.
  - Accessing or sharing precise geolocation information.

- Is the sharing of the data necessary or useful for an important business purpose (*e.g.*, to enhance advertising effectiveness)? ☐ Yes ☐ No
- Is the sharing of the data disclosed to the user (in the privacy policy or otherwise)? ☐ Yes ☐ No

☐ **Is the data deleted when it is no longer needed to fulfill the purpose for which it was collected?** ☐ **Yes** ☐ **No**

☐ **Does the app change or circumvent the user's default settings or privacy settings on their browser?** ☐ **Yes** ☐ **No**

If YES …

- Is there a functional reason for this and does this occur only after the user has given express consent? ☐ Yes ☐ No

  Note: Absent a functional reason to change default settings, ask if such an initiative reflects your brand's consumer values even with consent.

☐ **What is the default privacy setting for the app?**

- Is the default not to collect personally identifiable information? ☐ Yes ☐ No
- Is the default to automatically collect device information, like IP address, UDID; etc.? ☐ Yes ☐ No
- Does the app require opt-in consent in order to collect personal information? ☐ Yes ☐ No

☐ **Is any data collected by the app collected directly by the toy company?** ☐ **Yes** ☐ **No**

If YES …

- You are responsible for advising the consumer about privacy practices, in whole or in part.

Direct, Targeted and Behavioral Advertising

A variety of laws, like CAN-SPAM and the Telephone Consumer Protection Act, may apply to mobile app activities. In addition, there has been increasing government scrutiny relating to online behavioral advertising, or targeted advertising, by mobile apps. Federal legislative efforts to implement a "Do Not Track" standard for mobile apps have stalled, but self-regulatory associations, such as the Digital Advertising Alliance and Network Advertising Initiative, have released their own guidelines governing online and mobile data collection. California recently amended its Online Privacy Protection Act (A.B. 370) to require website operators and online services to disclose whether they or any third parties that collects personal information comply with "do not track" signals from Internet browsers. That law took effect on January 1, 2014.

Toy companies should regularly review and update this section as regulators and the advertising industry continue to address advertising and marketing for mobile apps.

☐ **Is non-personal information collected for purposes of identifying unique users, time spent on the app, or other information used to gauge interest and effectiveness?**	☐ **Yes**	☐ **No**
If YES …		
– Is this disclosed in the mobile app privacy policy?	☐ Yes	☐ No
☐ **Is non-personal information collected for purposes of analysis used to segment audiences for purposes of advertising?**	☐ **Yes**	☐ **No**
If YES ...		
– Is this disclosed in the mobile app privacy policy? *Note: The line between audience segmentation and behaviorally targeted advertising may be difficult to draw, and the recent COPPA revisions prohibit creation of an audience segment such as "under 13."*	☐ Yes	☐ No
☐ **Does the app collect information for purposes of offering targeted or behavioral advertising or serve targeted or behavioral advertisements?**	☐ **Yes**	☐ **No**
If YES ...		
– Does the app obtain the adult user's express prior consent before collecting information in order to send the advertisement or commercial message? *Note: If the app collects data from, or markets to, kids, the member company should ensure compliance with the Mobile Apps Directed to Children checklist in this document.*	☐ Yes	☐ No
– Does the app allow users to opt out of receiving behaviorally targeted advertising?	☐ Yes	☐ No
☐ **Does the app collect personal information, such as a phone number, for telemarketing purposes?**	☐ **Yes**	☐ **No**
If YES ...		
– Does the app obtain the user's express prior consent before collecting the personal information for this purpose?	☐ Yes	☐ No

Privacy Policy Considerations

To properly disclose data practices to app users, the privacy policy must identify what information is collected via the app, how it is used, whether it is combined with other data, and with whom it is shared. For toy company apps, the company should have agreements in place indemnifying it from the app developer's data privacy; the company's privacy policy should also be available to the user at the time of purchase or download. Recognizing that app initiatives may be brought to the toy company by advertising agencies, and the toy company may never have direct contact, much less contracts, in place with the app providers, any agreements with advertising agencies should require compliance with laws and best practices and indemnify and hold the toy company harmless from the app developer's data privacy practices.

☐ **Is a written app privacy policy available to the user prior to download?**	☐ **Yes**	☐ **No**
☐ **Is the privacy policy reasonably easy to read on a mobile device?** *Note: The FTC encourages the use of icons and short statements; however, there is no standardized guidance on this point, in part because the potential for inconsistency or failure to disclose information that a plaintiff or regulator might deem material could result in legal liability.*	☐ **Yes**	☐ **No**
☐ **Does the app's privacy policy disclose the following information:**	☐ **Yes**	☐ **No**
– What personal and non-personal information is collected, by whom, how it is used, and with whom is it shared.	☐ Yes	☐ No
– What information is collected automatically (e.g., unique device ID, IP address, information about the way the application is used).	☐ Yes	☐ No
– Whether the app collects precise, real time location (geolocation) information.	☐ Yes	☐ No
– What third parties have access to users' information and who the information may be transferred to.	☐ Yes	☐ No
– Whether the app is supported by advertising, and thus collects data to help the app serve advertisements.	☐ Yes	☐ No
– The users' opt-out rights.	☐ Yes	☐ No
– That the app does not knowingly collect data from, or market to, children under the age of 13. *Note: If the app collects data from, or markets to, kids, the member company should ensure compliance with the Mobile Apps Directed to Children checklist in this Guidance.*	☐ Yes	☐ No
– Contact information for the "operator" (the entity principally responsible for data collection through the app). *Note: Recent revisions to the COPPA Rule require all operators of a kid-directed website or online service, including apps, to provide contact information for all operators in the privacy policy, but allow designation of one operator to respond to questions about privacy practices.*	☐ Yes	☐ No
– General security precautions for collected data.	☐ Yes	☐ No

☐ **Does the app's privacy policy confirm that user consent will be obtained for any material changes to the data policies and practices affecting previously collected data?**	☐ **Yes** ☐ **No**
☐ **If the app is offered by an independent party, is the app's privacy policy in line with the privacy commitments of the toy company's privacy policy?**	☐ **Yes** ☐ **No**
☐ **Does the app comply with the policies and requirements of the platform that supports the app (*e.g.*, Apple, Android, Facebook, Intel, Microsoft)?**	☐ **Yes** ☐ **No**
☐ **Does the app run on a social networking site?** **If YES ...** – Is the privacy policy consistent with applicable developer policies for the social networking site (*e.g.*, Facebook, Foursquare, etc.)? – If the app allows the consumer's name or likeness to be used in connection with ads, is opt-in consent obtained? – Is the app intended for teens or adults if the social networking site is not suitable for children under 13?	☐ **Yes** ☐ **No** ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No

Data Security

Companies transmitting, receiving, processing or storing personally identifiable information must adopt security measures appropriate to the sensitivity of the information collected via the app. They should conduct periodic risk assessments and update security measures and practices periodically.

☐ **Is data, including authentication data, session data, or personal information (including e-mail addresses, passwords, etc.) encrypted in transit?** ☐ **Yes** ☐ **No**

If YES …

– What technology is used (*e.g.*, SSL/TLS)? ☐ Yes ☐ No

If NO …

– Have you considered risks of data leakage or access? ☐ Yes ☐ No

☐ **Is user data (e-mail addresses, user names, passwords, etc.) stored in encrypted format?** ☐ **Yes** ☐ **No**

Note: The FTC in a recent complaint asserted that storage of e-mail addresses and passwords in clear text format reflected inadequate security and contributed to a significant data breach. A recent amendment to California's data breach notification law (Cal. Civ. Code § 1798.82) that took effect on January 1, 2014 expands the definition of "personal information" to include a user name or email address, in combination with a password or security question and answer that would permit access to an online account.

☐ **Is sensitive information (such as credit card information) collected or stored via the app?** ☐ **Yes** ☐ **No**

If YES ...

– What mechanism (*e.g.*, two-factor authentication, application-specific passwords, encryption) is used to safeguard the data?

Consumer Protection Considerations

These general considerations relating to app content apply to a toy company's participation in both in-app advertisement and the development of mobile apps.

☐	**Are ads distinguishable to the reasonable consumer from app content such as games or marked in some way to indicate they are ads?**	**☐ Yes**	**☐ No**
☐	**Does the app include bumpers or interstitials to notify the user that s/he is leaving the app to go to the member company's or third-party website (where a different privacy policy may apply)?**	**☐ Yes**	**☐ No**
☐	**Does the app allow for in-app purchases?**	**☐ Yes**	**☐ No**
	If YES ...		
	– Are fees, and the basis of charges (*e.g.*, per game) clear?	☐ Yes	☐ No
	– Does the app include a notification button or other feature that notifies the user every time they will be charged for an in-app purchase?	☐ Yes	☐ No
	– Must a password be entered before each purchase?	☐ Yes	☐ No
	– Are charges capped absent additional action on the part of the consumer?	☐ Yes	☐ No
	If NO …		
	– Can the consumer opt-out at any time?	☐ Yes	☐ No
☐	**For mobile sweepstakes and contests, can the user send an SMS text to enter the mobile-based promotion?**	**☐ Yes**	**☐ No**
	If YES ...		
	– Is express consent obtained from the user to enter online?	☐ Yes	☐ No
	– Is there a disclosure that "messaging and data rates may apply"?	☐ Yes	☐ No
	– If there a charge or "premium fee" to send the text message entry, is the fee disclosed and consent obtained?	☐ Yes	☐ No
	– Are there alternative methods of entry (AMOE), such as a free mail-in entry form or online entry method for sweepstakes?	☐ Yes	☐ No

Intellectual Property Considerations

Regardless of who develops the app, intellectual property rights should be addressed. If the toy company develops the app, it should establish its IP rights to the app contractually, and determine whether a unique trademark for the app should be registered.

☐ **Does the app implicate any intellectual property rights?**	**☐ Yes**	**☐ No**
If YES … for in-app advertisements:		
– Does the app developer provide global IP clearance for images, video, music, trademarks, logos, software, etc.?	☐ Yes	☐ No
If YES … for an app developed by the toy company:		
– Do contracts establish that the toy company owns or has unrestricted rights to use the IP globally?	☐ Yes	☐ No
☐ **Does the app permit file-sharing of photos, videos, music, etc.?**	**☐ Yes**	**☐ No**
If YES …		
– Is the app directed to adults?	☐ Yes	☐ No
– Do terms and conditions of filing-sharing clarify IP issues?	☐ Yes	☐ No

Contractual Protections

The following questions apply to both a toy company's participation with in-app advertisement and the development of mobile apps. The member company should get indemnification from the third party developer in apps it develops, and seek indemnifications from advertising agencies related to in-app advertising initiatives. Independent due diligence on the app provider may also be advisable.

☐	**Has the developer provided a Statement of Work ("SOW") or other agreement outlining the app activity?**	☐ **Yes**	☐ **No**
☐	**Does the SOW or agreement require:**		
	– General compliance with all applicable laws and regulations?	☐ Yes	☐ No
	– Adherence to the CAN-SPAM Act?	☐ Yes	☐ No
	– Adherence to the Telephone Consumer Protection Act?	☐ Yes	☐ No
	– Adherence to the Mobile Marketing Association's Mobile Application Privacy Policy Framework?	☐ Yes	☐ No
	– Adherence to the CTIA's Best Practices and Guidelines for Location-Based Services?	☐ Yes	☐ No
	– Adherence to best practices for OBA?	☐ Yes	☐ No
☐	**Does the agreement include representations and warranties related to privacy, data security and intellectual property?**	☐ **Yes**	☐ **No**
☐	**Does the agreement hold harmless and indemnify the toy company for IP, privacy, data security and other violations of legal and contractual commitments?**	☐ **Yes**	☐ **No**
☐	**Is the toy company included as an additional insured on the app developer's and ad agency's insurance policy, with coverage for advertising liability and privacy/data security breaches?**	☐ **Yes**	☐ **No**
☐	**Does the scope of the indemnification expressly include investigations by the FTC and state AG's other regulatory bodies, as well as private litigation?**	☐ **Yes**	☐ **No**

Mobile Apps Directed to Children

The FTC has indicated that mobile apps directed to children are subject to COPPA. In its final COPPA Rule, the FTC revised the definition of personally identifiable information (PII) to include (among other things) persistent identifiers, such as an Internet Protocol (IP) address, a customer number held in a cookie, or a unique device identifier (UDID), implicating additional instances where verifiable parental consent must be obtained before collecting the PII. In addition, precise geolocation information as well as photos, videos and audio files collected at a child-directed website, service or app are now *per se* "personal information." Collection at child-directed websites, online services or apps requires verifiable parental consent. Thus, while the basic considerations outlined above apply to all apps, special concerns apply to child-directed apps. Remember: while the FTC applies a totality of the circumstances test in determining when an app is directed to children, appearance of animated characters may result in an assumption that the app is child-directed. Brand and marketing plans and demographic data may be helpful in establishing the actual target audience. However, other jurisdictions might look principally at whether the app "appeals" to children to determine if it is child-directed. These factors should be considered in evaluating the target audience.

☐ **Is the app content directed to children under the age of 13?** ☐ **Yes** ☐ **No**

If YES …

- Obtain "verifiable parental consent" (VPC) before collecting, using, or disclosing personally identifiable information from kids (*e.g.*, full name, address, e-mail, telephone number, geolocation information or any other information that would allow someone to identify or contact the child) or tracking them across other websites to serve advertising.
- Provide direct notice to parents of what information is collected online from children, how such information is used, and the disclosure practice unless COPPA exceptions apply.
- Allow parents to opt-out or limit the collection, use, and disclosure of their children's personal information, and access personal information about their child that you collect via the app.
- Where possible, limit the collection of personal information, as well as information that allows a child to be tracked across the Internet and over time.
- Assure that the content of the mobile app is age-appropriate.
- Do not use any part of the app to entice a child to divulge personally identifiable information by the prospect of a special game, prize, or other offer.
- Do not allow a link in a kid-directed app to a site or area not intended for children or not compliant with COPPA.
- Consider bumpers or interstitials if an app allows a child to visit another website.
- Do not allow in-app purchases or any other mobile payments to be made through the app without obtaining verifiable parental consent, establishing a cap on charges, or other mechanisms to limit the incurred charges.
- Require the app developer to comply with COPPA and CARU guidelines.

☐	**If app offerings are intended for adults but might appeal to kids, is there any age-gate, age-screen or other information collected at any point from the app (e.g., through a survey or registration for coupons) that would indicate how old the app user is?** **If YES …** – Use neutral age-screening and deny access to those under age 13 if the app is intended for older visitors. *Note: If the app permits collection of certain information such as birthdate in surveys, etc., use care as you may then have actual knowledge that you have collected information from someone under 13.* – Do not use leading language in age-screens such as "must be 13 or older"	**☐ Yes**	**☐ No**
☐	**Have you notified the app developer that the app is directed to children?**	**☐ Yes**	**☐ No**
☐	**Have you reviewed the terms of service and privacy policy offered by your service provider (app developer, analytic provider, etc.) to assess policies on children?**	**☐ Yes**	**☐ No**
	– Has the app developer provided contractual or other assurances of compliance with COPPA?	☐ Yes	☐ No
	– Do the service provider's policies establish that it understands requirements for children's privacy?	☐ Yes	☐ No
	– Does the service provider participate in privacy self-regulatory programs?	☐ Yes	☐ No

Questions and comments on this guidance document can be directed to info@toyassociation.org

1115 Broadway | Suite 400 | New York, NY 10010

T: 212.675.1141 | F: 212.633.1429

info@toyassociation.org | www.toyassociation.org