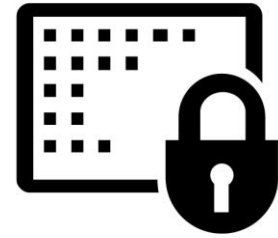




A service of the advertising industry and Council of Better Business Bureaus



Website Privacy Digest

CARU's role: The Children's Advertising Review Unit monitors and reviews advertising and websites directed to children for compliance with its guidelines. CARU initiates and receives complaints about advertising and online privacy practices, and determines whether such practices violate the program's standards. When it finds violations, it seeks changes through the voluntary cooperation of advertisers and Website operators.

CARU's Guidelines for Online Privacy Protection address concerns about the collection of personal data from children and other privacy-related practices on the Internet. Its provisions are consistent with the Children's Online Privacy Protection Act of 1998 (COPPA)¹, which was designed to protect children under the age of 13.

The Guidelines provide guidance on specific issues involving online data collection and other privacy-related practices by Website operators that target children under 13 years of age or that know or should know that a visitor is a child under 13 years of age. Since 2000, CARU has issued more than 200 decisions involving its online privacy guidelines and COPPA. Excerpts from several recent cases follow.

Age Screening

Relevant CARU Guideline:

Part I: Online Privacy Protection Guidelines, (b) Age-Screening/Hyperlinks

1. On Websites where there is a reasonable expectation that a significant number of children will be visiting, advertisers should employ age-screening mechanisms to determine whether verifiable parental consent or notice and opt-out is necessitated under the Data Collection provisions (see endnote for full text Online Protection Guidelines).¹
2. Advertisers should ask screening questions in a neutral manner so as to discourage inaccurate answers from children trying to avoid parental permission requirements.
3. Age-screening mechanisms should be used in conjunction with technology, *e.g.*, a session cookie, to help prevent underage children from going back and changing their age to circumvent age-screening.

DUNCAN ENTERPRISES
www.ilovetocreate.com
Case #5158 (03/30/10)

¹ Children's Online Privacy Protection Act (15 U.S.C. 6501 et seq.).

The Operator's arts and crafts products and its Website were advertised in a magazine geared toward children ages eight and up. The Website collected personally identifiable information ("PII") from visitors and did not have an age screening process.

CARU Findings: CARU determined that Operators who advertise websites in child directed media should have a reasonable expectation that a significant number of children will be visiting and should employ age-screening mechanisms to determine whether verifiable parental consent or notice and opt-out is needed before collecting personal information.

ROBLOX

www.Roblox.com

Case #5137 (01/21/10)

A virtual world Website required registrants to choose either "Under 13" or "13 or Older" in its registration process. The icon that accompanied the "Under 13" age category was white and innocent looking whereas the icon for the "13 and Older" age category was red, wearing sunglasses and appeared fun and enticing.

If the registrant signed up as "Under 13," he was asked to create a username and password and asked to enter a parent's email address. The child could click the browser's back button and change his age selection and register using the "13 or Older" category where a parent's email was not requested.

CARU Findings: CARU determined that the use of non-neutral language, coupled with leading images, may encourage children younger than 13 who want to play an online game to misrepresent their age when registering.

CARU also determined that the Website was not in compliance with its guidelines because it did not employ a tracking mechanism (for example, a session cookie) to prevent a child from circumventing the age-screening process by hitting the browser's back button and re-registering as an "over 13" user.

E-Cards and Forward-to-a-Friend Emails

Relevant Legal Requirements:

In 2008, the Federal Trade Commission (FTC) revised its Frequently Asked Questions about COPPA on E-cards and forward-to-a-friend functions to clarify that any feature providing the opportunity to reveal any PII in the recipient's inbox or body of the message requires the Operator to obtain verifiable parental consent (rather than relying on the one-time exception to consent). It further stated that if a Website chooses to retain the recipient's email address until some point in the future (*e.g.*, until e-card is opened by the recipient, or if you allow the sender to indicate a date in the future when the e-card should be sent), you must collect the sender's parent's email address and provide notice and opt-out to the sender's parent *before* the e-card is sent.²

AMERICAN BEVERAGE COMPANY

www.littlehug.com

Case #5228 (09/28/10)

² See Website, <http://www.ftc.gov/privacy/coppafaqs>, COPPA FAQ, #44.

A beverage company's Website had an e-card feature. In the body of the card, a child was able to freely type a message and enter PII. The sender's parent was neither notified of this disclosure nor asked for permission before the e-card was sent.

CARU's Findings: Where a Website allows the sender to freely type her own message in the subject line or body of the e-card, it cannot take advantage of the COPPA one-time exception and must use a reliable method to obtain verifiable parental consent (e.g. a consent form to be signed by the parent and sent to the Operator by postal mail or facsimile).

BUILD-A-BEAR WORKSHOP

www.buildabear.com

Case #5123 (12/11/09)

A Website featuring children's toys had an e-card feature where a visitor could freely type a message in the card including PII such as a telephone number. A visitor could also choose a future date to send the e-card and be notified via email when the card was sent to the recipient.

CARU's Findings: CARU determined that where a Website allows the sender to freely type her own message in the subject line or body of the e-card, it cannot take advantage of the COPPA one-time exception and must use a reliable method to obtain verifiable parental consent.

CARU also determined that the Website could not retain the recipient's email address for longer than necessary to send the card. Where an e-card is not sent immediately, the Website must also collect the sender's parent's email address and provide notice and opt-out before the e-card is sent.

Allowing Children to Publically Post Personally Identifiable Information

Relevant CARU Guideline:

Part I: Online Privacy Protection Guidelines,
(a) Data Collection

4. Advertisers must obtain prior "verifiable parental consent" when they collect personal information (such as email addresses, screen names associated with other personal information, phone numbers or addresses) that will be publicly posted, thereby enabling others to communicate directly with the child online or offline, or when the child will be otherwise able to communicate directly with others.

GAMELOFT

www.gameloft.com

Case #5035 (06/17/09)

A Website that sold video games for cell phones contained a forum feature where children could post PII that could be read by other members.

CARU's Findings: CARU determined that Operators of Websites must obtain prior verifiable parental consent when they collect personal information that will be publicly posted or when the child will be able to communicate directly with others.

FLOW PLAY, INC.
www.ourWorld.com
Case# 4936 (11/20/08)

CARU reviewed an online game where players could share PII in a virtual world environment. The Website used a system that filtered PII in the chat and messaging areas of the Website. However, CARU noted that not all PII was filtered and a player could disclose a full name in the chat room and a telephone number in the internal messaging system.

CARU Findings: CARU determined the Website must use one of the more reliable methods to obtain verifiable parental consent before allowing children use these features or use a filtering system where no PII can be communicated among players.

CARTOON DOLL EMPORIUM LLC
cartoondollemporium.com
Case #4964 (01/22/2009)

Registered members of a social networking site could send friend requests to other players that included PII. Once a request was accepted, players could exchange PII, such as telephone numbers, through the internal messaging system.

The Website also collected a parent's email address and included a check-box to indicate consent during the registration process. However, the Operator did not actually contact the parent.

CARU Findings: CARU determined that because the Website allowed children to share PII with other players, it was obligated to obtain prior verifiable parental consent.

Regarding its method of obtaining consent, CARU determined that checking a box is not a reliable method of consent. COPPA requires that any method of consent be reasonably calculated to ensure that the person providing consent is the child's parent. In this case, the "consent" (i.e. checking a box) was requested during the registration process, which was completed by the child, rather than contacting the parent directly and using a reliable method such as credit card verification or a social security number.

Notice to a Parent

Legal Requirements:

COPPA:

§312.4 Notice³

³ Children's Online Privacy Protection Rule, 16 C.F.R. Part 312.

(1) Content of Notice to Parent

(i) All notices must state the following:

(A) That the operator wishes to collect personal information from the child;

(B) The information set forth in paragraph (b) of this section.

(ii) In the case of a notice to obtain verifiable parental consent under §312.5(a), the notice must also state that the parent's consent is required for the collection, use, and/or disclosure of such information, and state the means by which the parent can provide verifiable consent to the collection of information.

SMILEY MILEY/IMM STUDIO, INC.

www.MileyWorld.com

Case #4752 (11/12/07)

A child registering for a child-directed members-only fan site was asked for personal information including a first and last name and email address. The next step required valid credit card information and a parent's email address. After this information was submitted by the parent and the parent clicked on the "Join Now" button, the child's membership was active. At no time during the registration process was the parent informed that by giving his credit card information he was also consenting to the collection of his child's information.

Additionally, if a parent was not present during the first step of the registration process he would not know what information the child had already submitted. Once a child was registered she could go to her profile and submit additional PII such as telephone number to the Website and could immediately post PII in the chat rooms, and on other areas.

CARU Findings: CARU determined that the Website did not provide adequate notice to parents. When parents provided their credit card information for payment of membership dues, they were not informed that they were also consenting to the collection and disclosure of their child's PII.

ⁱ **The Guidelines for Online Privacy Protection**

(a) Data Collection

1. In collecting information from children under 13 years of age, advertisers should adhere to the following guidelines: Advertisers must clearly disclose all information collection and tracking practices, all information uses, and the means for correcting or removing the information. These disclosures should be prominent and readily accessible before any information is collected. For instance, on a Website where there is passive tracking, the

notice should be on the page where the child enters the site. A heading such as "Privacy," "Our Privacy Policy," or similar designation is acceptable if it allows an adult to click on the heading to obtain additional information on the site's practices concerning information collection, tracking and uses.

2. Advertisers should disclose, in language easily understood by a child, (a) why the information is being requested (e.g., "We'll use your name and email to enter you in this contest and also add it to our mailing list") and (b) whether the information is intended to be shared, sold or distributed outside of the collecting company.

3. Advertisers should disclose any passive means of collecting information from children (e.g., navigational tracking tools, browser files, etc.) and what information is being collected.

4. Advertisers must obtain prior "verifiable parental consent" when they collect personal information (such as email addresses, screen names associated with other personal information, phone numbers or addresses) that will be publicly posted, thereby enabling others to communicate directly with the child online or offline, or when the child will be otherwise able to communicate directly with others.

5. For activities that involve public posting, advertisers should encourage children not to use their full names or screen names that correspond with their email address, but choose an alias (e.g., "Bookworm," "Skater," etc.) or use first name, nickname, initials, etc.

6. Advertisers should not require a child to disclose more personal information than is reasonably necessary to participate in the online activity (e.g., play a game, enter a contest, etc.).

7. Advertisers must obtain prior "verifiable parental consent" when they plan to share or distribute personal information to third parties, except parties that are agents or affiliates of the advertiser or provide support for the internal operation of the Website and that have agreed not to disclose or use the information for any other purpose.

8. When an advertiser collects personal information only for its internal use and there is no disclosure of the information, the company must obtain parental consent, and may do so through the use of email, coupled with some additional steps to provide assurance that the person providing the consent is the parent.

9. When an advertiser collects and retains online contact information to be able to respond directly more than once to a child's specific request (such as an email newsletter or contest) but will not use the information for any other purpose, the advertiser must directly notify the parent of the nature and intended uses of the information collected, and permit access to the information sufficient to allow a parent to remove or correct the information.

10. To respect the privacy of parents, advertisers should not maintain in retrievable form information collected and used for the sole purpose of obtaining verifiable parental consent or providing notice to parents, if consent is not obtained after a reasonable time.

11. If an advertiser communicates with a child by email, there should be an opportunity with each mailing for the child or parent to choose by return email or hyperlink to discontinue receiving mailings.

(b) Age-Screening/Hyperlinks

1. On Websites where there is a reasonable expectation that a significant number of children will be visiting, advertisers should employ age-screening mechanisms to determine whether verifiable parental consent or notice and opt-out is necessitated under the Data Collection provisions above.
2. Advertisers should ask screening questions in a neutral manner so as to discourage inaccurate answers from children trying to avoid parental permission requirements.
3. Age-screening mechanisms should be used in conjunction with technology, *e.g.*, a session cookie, to help prevent underage children from going back and changing their age to circumvent age-screening.