COPPA - Children's Online Privacy Protection Act

How to comply with Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act, effective April 21, 2000, applies to the online collection of personal information from children under 13. The new rules spell out what a Web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent and what responsibilities an operator has to protect children's privacy and safety online.

The Federal Trade Commission staff prepared this guide to help you comply with the new requirements for protecting children's privacy online and understand the FTC's enforcement authority.

Who Must Comply

If you operate a commercial Web site or an online service directed to children under 13 that collects personal information from children or if you operate a general audience Web site and have actual knowledge that you are collecting personal information from children, you must comply with the Children's Online Privacy Protection Act.

- To determine whether a Web site is directed to children, the FTC considers several factors, including the subject matter; visual or audio content; the age of models on the site; language; whether advertising on the Web site is directed to children; information regarding the age of the actual or intended audience; and whether a site uses animated characters or other child-oriented features.
- To determine whether an entity is an "operator" with respect to information collected at a site, the FTC will consider who owns and controls the information; who pays for the collection and maintenance of the information; what the pre-existing contractual relationships are in connection with the information; and what role the Web site plays in collecting or maintaining the information.

Personal Information

The Children's Online Privacy Protection Act and Rule apply to individually identifiable information about a child that is collected online, such as full name, home address, email address, telephone number or any other information that would allow someone to identify or contact the child. The Act and Rule also cover other types of information -- for example, hobbies, interests and information collected through cookies or other types of tracking mechanisms -- when they are tied to individually identifiable information.

Basic Provisions

Privacy Notice

Placement

An operator must post a link to a notice of its information practices on the home page of its Web site or online service and at each area where it collects personal information from children. An operator of a general audience site with a separate children's area must post a link to its notice on the home page of the children's area.

The link to the privacy notice must be clear and prominent. Operators may want to use a larger

font size or a different color type on a contrasting background to make it stand out. A link in small print at the bottom of the page -- or a link that is indistinguishable from other links on your site -- is not considered clear and prominent.

Content

The notice must be clearly written and understandable; it should not include any unrelated or confusing materials. It must state the following information:

- The name and contact information (address, telephone number and email address) of all operators collecting or maintaining children's personal information through the Web site or online service. If more than one operator is collecting information at the site, the site may select and provide contact information for only one operator who will respond to all inquiries from parents about the site's privacy policies. Still, the names of all the operators must be listed in the notice.
- The kinds of personal information collected from children (for example, name, address, email address, hobbies, etc.) and how the information is collected -- directly from the child or passively, say, through cookies.
- How the operator uses the personal information. For example, is it for marketing back to the child? Notifying contest winners? Allowing the child to make the information publicly available through a chat room?
- Whether the operator discloses information collected from children to third parties. If so, the operator also must disclose the kinds of businesses in which the third parties are engaged; the general purposes for which the information is used; and whether the third parties have agreed to maintain the confidentiality and security of the information.
- That the parent has the option to agree to the collection and use of the child's information without consenting to the disclosure of the information to third parties.
- That the operator may not require a child to disclose more information than is reasonably necessary to participate in an activity as a condition of participation.
- That the parent can review the child's personal information, ask to have it deleted and refuse to allow any further collection or use of the child's information. The notice also must state the procedures for the parent to follow.

Direct Notice to Parents

Content

The notice to parents must contain the same information included on the notice on the Web site. In addition, an operator must notify a parent that it wishes to collect personal information from the child; that the parent's consent is required for the collection, use and disclosure of the information; and how the parent can provide consent. The notice to parents must be written clearly and understandably, and must not contain any unrelated or confusing information. An operator may use any one of a number of methods to notify a parent, including sending an email message to the parent or a notice by postal mail.

Verifiable Parental Consent

Before collecting, using or disclosing personal information from a child, an operator must obtain verifiable parental consent from the child's parent. This means an operator must make reasonable efforts (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child receives notice of the operator's information practices and consents to those practices.

Until April 2002, the FTC will use a sliding scale approach to parental consent in which the required method of consent will vary based on how the operator uses the child's personal information. That is, if the operator uses the information for internal purposes, a less rigorous method of consent is required. If the operator discloses the information to others , the situation

presents greater dangers to children, and a more reliable method of consent is required. The sliding scale approach will sunset in April 2002 subject to a Commission review planned for October 2001.

Internal Uses

Operators may use email to get parental consent for all internal uses of personal information, such as marketing back to a child based on his or her preferences or communicating promotional updates about site content, as long as they take additional steps to increase the likelihood that the parent has, in fact, provided the consent. For example, operators might seek confirmation from a parent in a delayed confirmatory email, or confirm the parent's consent by letter or phone call.

Public Disclosures

When operators want to disclose a child's personal information to third parties or make it publicly available (for example, through a chat room or message board), the sliding scale requires them to use a more reliable method of consent, including:

- getting a signed form from the parent via postal mail or facsimile;
- accepting and verifying a credit card number in connection with a transaction;
- taking calls from parents, through a toll-free telephone number staffed by trained personnel;
- email accompanied by digital signature;

But in the case of a monitored chat room, if all individually identifiable information is stripped from postings before it is made public -- and the information is deleted from the operator's records -- an operator does not have to get prior parental consent.

Disclosures to Third Parties

An operator must give a parent the option to agree to the collection and use of the child's personal information without agreeing to the disclosure of the information to third parties. However, when a parent agrees to the collection and use of their child's personal information, the operator may release that information to others who uses it solely to provide support for the internal operations of the website or service, including technical support and order fulfillment.

Exceptions

The regulations include several exceptions that allow operators to collect a child's email address without getting the parent's consent in advance. These exceptions cover many popular online activities for kids, including contests , online newsletters , homework help and electronic postcards .

Prior parental consent is not required when:

- an operator collects a child's or parent's email address to provide notice and seek consent;
- an operator collects an email address to respond to a one-time request from a child and then deletes it;
- an operator collects an email address to respond more than once to a specific request -- say, for a subscription to a newsletter. In this case, the operator must notify the parent that it is communicating regularly with the child and give the parent the opportunity to stop the communication before sending or delivering a second communication to a child;
- an operator collects a child's name or online contact information to protect the safety of a child who is participating on the site. In this case, the operator must notify the parent

and give him or her the opportunity to prevent further use of the information;
- an operator collects a child's name or online contact information to protect the security or liability of the site or to respond to law enforcement, if necessary, and does not use it for any other purpose.

October 2001/April 2002

In October 2001, the Commission will seek public comment to determine whether technology has progressed and whether secure electronic methods for obtaining verifiable parental consent are widely available and affordable. Subject to the Commission's review, the sliding scale will expire in April 2002. Until then, operators are encouraged to use the more reliable methods of consent for all uses of children's personal information.

New Notice for Consent

An operator is required to send a new notice and request for consent to parents if there are material changes in the collection, use or disclosure practices to which the parent had previously agreed. Take the case of the operator who got parental consent for a child to participate in contests that require the child to submit limited personal information, but who now wants to offer the child chat rooms. Or, consider the case of the operator who wants to disclose the child's information to third parties who are in materially different lines of business from those covered by the original consent -- for example, marketers of diet pills rather than marketers of stuffed animals. In these cases, the Rule requires new notice and consent.

Access Verification

At a parent's request, operators must disclose the general kinds of personal information they collect online from children (for example, name, address, telephone number, email address, hobbies), as well as the specific information collected from children who visit their sites. Operators must use reasonable procedures to ensure they are dealing with the child's parent before they provide access to the child's specific information.

They can use a variety of methods to verify the parent's identity, including:

- obtaining a signed form from the parent via postal mail or facsimile;
- accepting and verifying a credit card number;
- taking calls from parents on a toll-free telephone number staffed by trained personnel;
- email accompanied by digital signature;
- email accompanied by a PIN or password obtained through one of the verification methods above.

Operators who follow one of these procedures acting in good faith to a request for parental access are protected from liability under federal and state law for inadvertent disclosures of a child's information to someone who purports to be a parent.

Revoking & Deleting

At any time, a parent may revoke his/her consent, refuse to allow an operator to further use or collect their child's personal information, and direct the operator to delete the information. In turn, the operator may terminate any service provided to the child, but only if the information at issue is reasonably necessary for the child's participation in that activity. For example, an operator may require children to provide their email addresses to participate in a chat room so the operator can contact a youngster if he is misbehaving in the chat room. If, after giving consent, a parent asks the operator to delete the child's information, the operator may refuse to allow the child to participate in the chat room in the future. If other activities on the Web site do not require the

child's email address, the operator must allow the child access to those activities.

Timing

The Rule covers all personal information collected after April 21, 2000, regardless of any prior relationship an operator has had with a child. For example, if an operator collects the name and email address of a child before April 21, 2000, but plans to seek information about the child's street address after that date, the later collection would trigger the Rule's requirements. In addition, come April 21, 2000, if an operator continues to offer activities that involve the ongoing collection of information from children -- like a chat room -- or begins to offer such activities for the first time, notice and consent are required for all participating children regardless of whether the children had already registered at the site.

Safe Harbors

Industry groups or others can create self-regulatory programs to govern participants' compliance with the Children's Online Privacy Protection Rule . These guidelines must include independent monitoring and disciplinary procedures and must be submitted to the Commission for approval. The Commission will publish the guidelines and seek public comment in considering whether to approve the guidelines. An operator's compliance with Commission-approved self-regulatory guidelines will generally serve as a Asafe harbor" in any enforcement action for violations of the Rule.

Enforcement

The Commission may bring enforcement actions and impose civil penalties for violations of the Rule in the same manner as for other Rules under the FTC Act. The Commission also retains authority under Section 5 of the FTC Act to examine information practices for deception and unfairness, including those in use before the Rule's effective date. In interpreting Section 5 of the FTC Act, the Commission has determined that a representation, omission or practice is deceptive if it is likely to:

- mislead consumers; and
- affect consumers' behavior or decisions about the product or service.

Specifically, it is a deceptive practice under Section 5 to represent that a Web site is collecting personal identifying information from a child for one reason (say, to earn points to redeem a premium) when the information will be used for another reason that a parent would find material -- and when the Web site does not disclose the other reason clearly or prominently.

In addition, an act or practice is unfair if the injury it causes, or is likely to cause, is:

- substantial;
- not outweighed by other benefits; and
- not reasonably avoidable.

For example, it is likely to be an unfair practice in violation of Section 5 to collect personal identifying information from a child, such as email address, home address or phone number, and disclose that information to a third party without giving parents adequate notice and a chance to control the collection and use of the information.

References: http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm