Filed electronically at https://secure.commentworks.com/ftccopparulereview

June 27, 2005

Donald S. Clark
Secretary
Federal Trade Commission
600 Pennsylvania Avenue, NW – Room 159-H (Annex C)
Washington, DC 20580

Re: COPPA Rule Review 2005, Project No. P054505

Dear Secretary Clark:

TRUSTe is pleased to respond to the Federal Trade Commission's ("the Commission") request for comments on its implementation of the Children's Online Privacy Protection Act, 15 U.S.C. 6501-6508, through the Children's Online Privacy Protection Rule ("COPPA Rule" or "Rule"), 16 C.F.R. Part 312.

In May 2001, the Commission approved TRUSTe's Children's Privacy Seal Program as a safe harbor under the COPPA Rule. We are proud to have received that designation. Hundreds of thousands of young children who are active online are protected by our program, which currently includes some of the most popular Web sites, including www.disney.go.com, www.kids.msn.com, and www.epals.com. We believe that the COPPA Rule has done a great deal to advance the Congressional goal of protecting children's privacy online, and we support its continuing implementation.

TRUSTe's Children's Privacy Seal Program

TRUSTe's Children's Privacy Seal Program is an essential piece of the COPPA enforcement picture. After we certify companies to our rigorous Program Requirements, we regularly monitor their online information practices and provide dispute resolution services when parents raise privacy concerns. Our seal holders' ongoing relationships with us ensure that they consistently comply with the COPPA Rule.

We see our Program as the first line of defense against violations of the COPPA Rule. It enables seal holders to resolve questions about regulatory compliance quickly with our guidance, and provides parents with a forum for resolving even minor complaints about use of their children's personal information. While our Program enables TRUSTe to bring strong enforcement measures to bear,

685 Market Street, Suite 560 ▪ San Francisco, CA 94105
1776 K Street NW, Suite 360 ▪ Washington, DC 20006 ▪ 202.835.9751
▪ fmaier@truste.org 415-530-3418 ▪ cbump@truste.org 415-520-3423
mlandesberg@truste.org 202-835-9751

including termination from our Program and referral to the Commission, we have rarely found this to be necessary. Companies join our Program precisely to demonstrate their commitment to children's online privacy and to COPPA compliance. We believe they should be recognized for their leadership.

The Commission's COPPA Five-Year Review

The Commission seeks comments on many specific provisions of the Rule. In comments submitted on February 14, 2005, we argued in support of indefinitely extending the "Sliding Scale" for obtaining verifiable parental consent under Section 312.5 of the Rule, even as we noted that our Children's Privacy Seal Program Requirements exceed that baseline standard. We refer the Commission to those comments as it considers the Rule more broadly. In response to the Commission's current Request for Public Comment, we focus on two issues raised by the Commission: (1) how to address issues raised by the Rule's "actual knowledge" standard where children whose personal information is subject to the Rule intentionally provide an age older than 12 to general audience Web sites; and (2) whether the Rule's safe harbor provisions have been sufficiently effective in advancing the Congressional goal of protecting children's online privacy.

Question 13: "Actual Knowledge" and General Audience Web Sites

The COPPA Rule applies, in part, to operators of commercial Web sites or online services that have "actual knowledge" that they are collecting or maintaining personal information from children under the age of 13. 16 C.F.R. Section 312.3. The Commission has requested comments on how to manage the situation where children falsely state that they are older than 12, in order to access "general audience" Web sites (i.e., those not "directed to children" within the meaning of the Rule). We have worked with our seal holders to understand the issues posed, and we are pleased to have consulted with the Commission staff as we developed guidance to address those issues. Our guidance document, *Complying with COPPA: TRUSTe's Guidance for General Audience Web Sites*, includes suggested steps companies can take to demonstrate they do not knowingly collect, or even want to collect, personal information from children under 13. We recommend, for example, that companies operating general audience sites that collect their users' ages implement a "bump-out" procedure

with session cookies, whereby young children who initially enter their true ages on online forms and are "bounced out" are then prevented from immediately returning to the same form and entering an age over 12. We also provide advice on other ways to discourage children from falsifying their ages. Although none of these measures is a "fool-proof" way of preventing children from misrepresenting their true ages, the guidance helps companies to demonstrate good-faith efforts not to violate the "actual knowledge" prong of the COPPA Rule. A copy of "*Complying with COPPA"* is attached in an Appendix to these comments.

Question 21: Safe Harbor

Section 312.10 of the Rule dictates the basic structure of self-regulatory safe harbor programs and is, therefore, of particular importance to us. We know that self-regulation currently plays an essential role in furthering children's privacy online, but we also believe that the Rule can be strengthened to significantly broaden industry participation in COPPA safe harbor programs.

We understand an effective safe harbor to be one which, if adhered to, (1) demonstrates that a member company is compliant with the regulation that created the safe harbor, and (2) functions as a defense in any enforcement action. Currently, Section 312.10 (a) of the Rule provides that an operator of a commercial Web site or online service "will be deemed to be in compliance" with the Rule if it is in compliance with Commission-approved self-regulatory guidelines. The Rule also states that membership in an approved self-regulatory program is a factor that the Commission will "take into account" in determining whether to open an investigation or file an enforcement action against the operator for alleged violations of the Rule. Section 312.10(b)(4). We believe that these provisions do not go far enough in motivating companies to join COPPA safe harbor programs.

We urge the Commission to consider amending Section 312.10 to provide that membership in good standing in a Commission-approved safe harbor program is an affirmative defense to an enforcement action by the Commission for alleged violations of the Rule. Changing the Rule in this way will provide a clear incentive for companies to join safe harbor programs, thereby expanding the number of companies taking advantage of the guidance and best practices offered by safe harbors as well as enhancing parents' ability to obtain redress in the event their children's personal information is misused. Providing an affirmative defense will surely lead to more widespread adoption of COPPA safe harbor programs and thus broaden the protection of children's online privacy, as Congress intended when it enacted the Children's Online Privacy Protection Act in 1998.

Conclusion

We appreciate this opportunity to share our views with the Commission. We believe that, in almost all respects, the COPPA Rule is working well, and we look forward to assisting the Commission as it works to strengthen the Rule to further protect children's online privacy.

Signed: Martha Landesberg, Senior Policy Advisor, TRUSTe

About TRUSTe

TRUSTe is the leading online privacy brand. As an independent, nonprofit organization, TRUSTe is dedicated to enabling individuals and organizations to establish trusting relationships based on respect for personal identity and information in the evolving networked world. Founded in 1997, today TRUSTe runs the largest and award-winning global privacy certification and seal program, with more than 1,500 Web sites certified throughout the world, including those of AOL, Microsoft, IBM, Nationwide and The New York Times. Its seal programs are certified as safe harbors for the Children's Online Privacy Protection Act (COPPA) and the EU Safe Harbor Framework. Information about all TRUSTe programs may be viewed at our web site at http://www.truste.org.

TRUSTe's programs have evolved since its inception to reflect changes in law, technology, industry practices and consumer needs. For example, TRUSTe has introduced Wireless Privacy Principles and Implementation Guidelines, and Security Guidelines for Privacy Professionals. Further, TRUSTe has proven expertise in legitimate email and is working on several fronts to further best practices in electronic mail. Our License Agreement now includes program requirements covering Licensees' email practices. TRUSTe also significantly contributes to anti-spam efforts by operating an Independent Trust Authority ("ITA") for email, most specifically as the certification and enforcement authority for Ironport's Bonded Sender program.

For further information, please contact: Fran Maier, Executive Director & CEO, at 415-520-3418, email: fmaier@truste.org; Cathy Bump, Vice President of Policy and Legal, at 415-520-3423, email cbump@truste.org; or Martha Landesberg, Senior Policy Advisor, at 202-83-9751; email mlandesberg@truste.org.

APPENDIX

Complying with COPPA: TRUSTe's Guidelines for General Audience Web Sites

Overview:

In April 2000, the Children's Online Privacy Protection Act (COPPA) became a law that regulates the business practices of gathering personal data online from children under 13. TRUSTe currently offers special Children's Privacy program for Web sites that are geared towards children under 13. In addition, all general audience Web sites that are part of the TRUSTe Privacy Seal program will need to be aware of COPPA's impact on their own business practices and ensure that they are in compliance with the law.

TRUSTe has created the following guidelines for our licensees. These guidelines apply to general audience Web sites that are not targeted towards users under the age of 13, but trigger COPPA oversight by having actual knowledge of the age of the user through the collection of the user's age, date of birth, or age revealing demographic questions. These guidelines reflect legal requirements, as well as best practices that we have developed to further protect children in the online world and provide predictability and continuity for companies.

Our aim with this document is straightforward: To demystify COPPA by giving Web sites guidance on how to comply with the law. These guidelines should help you better understand how general audience Web sites can meet TRUSTe's Privacy Program requirements prior to the collection of personally identifiable information from children under 13.

Guidelines:

1. Does the site need to collect age data?

COPPA does not require general audience Web sites to verify the age of all of their users. It simply requires Web sites that have actual knowledge of the user's age to obtain parental consent prior to the collection of personally identifiable information from children under 13. TRUSTe advises Web sites to consider the following when discerning the need to collect user age data:

a. If the site is collecting data for demographic purposes only, Web site operators are encouraged to ask demographic questions that do not force users to reveal their age.

<u>Examples of Non-Age Revealing Demographic Questions:</u>
What is your marital status?
What are your hobbies?

<u>Example of Age Revealing Demographic Questions:</u>
What grade are you in?
What is the highest level of education completed?
How old are you?

b. Tie the collection of age or birth date with a transaction where credit card information is required.

c. Collect birth date without the year of birth. This is especially useful for sites that want to send a special offer to the user on their birthday.

2. How does the operator plan to use the information that it collects?

If the information used falls under one of the email exceptions (see the Children's Online Privacy Protection Rule, 16 CFR Part 312) then only parental notification may be required. If the information is used for internal purposes, the operator can use the email "plus" means of parental consent.

TRUSTe defines email "plus" as gaining parental consent via email plus taking an additional step to verify that the parent has given consent. Web sites must also allow the parent to revoke consent at a later date. Forms of added verification could include requesting the parent to provide a mailing address or phone number. The site will then need to follow up with a letter sent via postal mail or with a phone call to verify that the parent has given consent and explain to the parent that consent can be revoked at any time. Web sites should consider the following:

a. Can the operator limit the use of the child's information so it falls within one of the email exceptions?

b. Can the operator limit the use of the child's information to internal purposes, thus allowing the email "plus" means of consent?

c. Can the operator offer the child access to content that does not require the collection of personally identifiable information?

d. Does the operator need to collect personally identifiable information from the user to allow them to utilize the site?

If the answer is "yes" to any of the above questions, operators should prevent false age data by creating a two step registration process where age is collected first. Under this process, if a user indicates that her age is under 13, she should be directed to a form that asks for her parent's email address and indicates that site use will be limited to areas that do not require personally identifiable information until verifiable parental consent is obtained. Alternatively, if the user indicates she is over 13, then she can proceed with the registration process as normal.

Note if an operator does not receive parental consent, the operator must delete the information collected from the child from its databases unless it falls under an email exception.

3. How does the site encourage users to not falsify their age?

If the site wants to collect age from users 13 and up but does not want to handle personally identifiable information from children under 13, then age needs to be asked through methods that do not encourage the user to falsify her age. Consider the following methods of encouraging users to tell the truth:

a. Sites should set "session cookies." A session cookie is a cookie that expires when the user chooses to close their browser to exit from the Internet.

b. If the operator needs to alert users that age is a factor – i.e. "You need to be at least 13 to use this site" – then the operator needs to place a session cookie that does not allow the user to re-access the registration page to change their age. By placing session cookies, the Web site will better prevent under age users from going back to the registration page to falsify their age. The alert should only appear after the user has entered her age, not before. For example, there should not be a statement on the form

that is collecting personally identifiable information that alerts the user that she needs to be at least 13 years old to use the site.

c. When the operator is unable to set a session cookie, operators should not indicate to the user that age is a factor as this could encourage the user to go back and change her age. Web sites can direct users that are self-identified as under 13 to a page that says "Thank you for your interest in our site but we are unable to accept your registration at this time."

d. Operators should not construct a "veil of ignorance." There are two primary examples of this practice. First, sites should not use age range boxes or drop down year of birth boxes that do not reflect the spirit of COPPA. To live up to the spirit of COPPA, the first age range that is offered should be "under 13" and users should be able to choose their correct birth year if the operator uses drop down boxes to collect birth date. Second, operators should not collect age by asking age revealing questions such as grade-level.

4. How is the site addressing public postings?

Operators that provide a means for users to publicly post personally identifiable information, but do not collect age data, should include information on how their site addresses public postings in their privacy policy. Specifically, their policy should highlight that if they learn a user under 13 is publicly posting or sharing personally identifiable information, then the user will be blocked from accessing these areas of the site.

This policy will need to be disclosed in the operator's privacy statement to demonstrate that measures are being taken to protect the child from continuing to publicly post personally identifiable information to third parties without their parent's verifiable consent. Forms of public postings include message boards, forums, chat, e-cards, free email addresses, and tell-a-friend features.

5. How does the site delete users' personally identifiable data from its database?

All operators should have an internal policy that requires it to delete personally identifiable data from its databases if it learns a user under the age of 13 has submitted personally identifiable information to the site without parental consent. This internal policy does not need to be disclosed in the privacy statement.

Note that an operator that has actual knowledge of the user's age and wants to simply say they will delete any personally identifiable information collected from users under 13 is not considered to have met TRUSTe's requirements for compliance with COPPA.

For More Information:

If you have any questions regarding compliance with the Children's Online Privacy Protection Act or the TRUSTe Privacy Seal program, please contact your TRUSTe account manager or visit the TRUSTe Web site at www.truste.org.