June 11, 1999

Donald S. Clark, Secretary
Federal Trade Commission
Room 159
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: *Children's Online Privacy Protection Rule -- Comment, P994504*

Dear Secretary Clark:

On behalf of the State of New York and the Attorneys General of the States of Alabama, Arizona, California, Florida, Georgia, Hawaii[1], Illinois, Indiana, Kansas, Maryland, Nevada, Ohio, Oklahoma, Tennessee, Vermont, and Washington ("the Attorneys General"), I wish to thank you for the opportunity to comment on the Rule proposed by the Federal Trade Commission ("FTC" or "Commission"), pursuant to Section 1303 of the Children's Online Privacy Protection Act of 1998 ("COPPA" or "Act"). The State Attorneys General are vitally concerned about the issue of online privacy, and in particular children's privacy, as are parents across our States. We commend the

[1] Georgia is represented by the Administrator of the Fair Business Practices Act ("Administrator"). The Administrator, who is not part of the State Attorney's General Office, is statutorily authorized to undertake consumer protection functions, including the civil and criminal investigation of Internet and financial identity fraud, and to accept or reject any Assurances of Voluntary Compliance of behalf of the State of Georgia. Hawaii is represented by its Office of Consumer Protection, an agency which is not a part of the State Attorney General's Office, but which is statutorily authorized to undertake consumer protection functions, including legal representation of the State of Hawaii. For the purposes of these comments, the entire group will be referred to as the "Attorneys General," and such designation, as it includes Hawaii, refers to the Executive Director of the State of Hawaii Office of Consumer Protection, and, as it includes Georgia, refers to the Administrator of the Fair Business Practices Act.

Commission for its leadership in addressing these important concerns and support final adoption of the proposed Rule.

I. GENERAL COMMENTS:

A. The Role of State Attorneys General

Protecting the health, safety, and welfare of our citizens historically has been, and remains today, among the core duties of the State Attorneys General. To fulfill that critical mission, we have worked independently and, where appropriate, with the Commission, to combat consumer fraud, illegal conduct, and invasions of privacy that pose a serious threat to the well-being of our citizens, regardless of either the violator's place of origin or the medium employed. These law enforcement efforts are important to the welfare of our citizens. They also foster the continued growth of e-commerce by bolstering consumer confidence in the Internet.

Existing State consumer protection statutes provide critical safeguards for our citizens in both the traditional marketplace and the new realm of the Internet, and we will continue to enforce these laws vigorously. Where federal laws are enacted to supplement these core protections, we favor measures that permit enforcement by both the federal government and the State Attorneys General, as is the case under COPPA. As such, we believe that this statute can serve as an effective model for future federal/State cooperation on Internet law enforcement matters.

B. The Explosive Growth of Online Commerce and Information Collection

The Internet is of growing importance to the individual and corporate citizens of our States. According to Forrester Research, Inc., the percentage of North American households with Internet access will nearly double between 1998 and 2003. The total number of web users globally is projected to grow from 16.1 million in 1995, to nearly 500 million by 2003. Over the last three years,

the number of commercial transactions occurring via the Internet has also skyrocketed. The total volume of Internet retail sales has grown from about $3 billion in 1996 to nearly $8 billion in 1998. During the 1998 holiday season, Internet retail sales reached more than $3 billion, nearly triple the amount for the same period in 1997. It is projected that this annual retail sales figure will jump to more than $108 billion in 2003, with nearly 40 million U.S. households shopping via the Internet in five years.

Accompanying this explosion in online commerce is a parallel expansion in the online collection of consumers' personal identifying information. This information is obviously valuable to businesses, who use it to market goods and services. Moreover, in the absence of adequate digital mechanisms to verify identity, sensitive personal information is also used to check a consumer's identity. Widespread collection of this information, in turn, increases the risk that personal data will be used in crimes of identity theft.

C. Consumer Concern About Online Privacy

Public surveys indicate that consumer concern about online privacy is so acute as to threaten the continued growth of the Internet's global marketplace. A 1998 poll conducted by Business Week/Harris found that 78 percent of current Internet users would use the Internet more often if more robust privacy protections were in place. The same poll also indicated that more than half of those surveyed want the government to pass laws restricting the collection and use of personal information on the Internet.

These concerns are particularly heightened with respect to the collection of personal identifying information from children. As Dr. Alan Westin noted in his testimony before the Commission during its 1997 Public Workshop on Consumer Information Privacy, 97 percent of

parents whose children use the Internet believe that websites should not sell or rent personal information relating to children. Dr. Westin further reported that 72 percent of parents object to websites that request a child's name and address when the child registers at the site, even if such information is used only by the website itself.

Despite this strong belief on the part of the public that online information collection from children should be carefully controlled, a study prepared by Commission Staff and presented to Congress in 1998 found that a startlingly high percentage of websites were collecting personal identifying information from children, while providing little or no explanation about how such information would be used. Specifically, the FTC found that:

1. As many as 89 percent of children's sites surveyed collected personal identifying information from children.

2. Only 46 percent of children's sites surveyed contained any disclosure of information collection and use practices.

3. Only 24 percent of children's sites surveyed contained a comprehensive privacy policy.

4. Only 23 percent of children's sites surveyed warned children to get their parents' consent before providing personal identifying information.

5. Fewer than 10 percent provided for some type of parental control over the collection of information from children.

In short, the FTC's study demonstrated that online practices did not square with parental concerns about how businesses should collect information from children. Although it is too early to tell whether self-regulation will provide effective protections for other types of online interactions, the survey results rightfully led the FTC to conclude that government intervention was necessary with respect to children's online privacy.

D. Flexible Self-Regulation with Regulatory Oversight and Enforcement

We believe that COPPA embodies an approach to regulation that is particularly well suited to the quickly-changing terrain of the Internet. The statute sets forth baseline standards for protecting children's privacy. Working within these standards, industry can develop mechanisms for complying with statutory and regulatory requirements, which, if approved by the Commission, will create a safe harbor. We support this approach because it is results-oriented, rather than merely proscriptive. It provides industry with an opportunity to propose alternative mechanisms for efficiently complying with COPPA, instead of imposing one-size-fits-all solutions upon a rapidly changing segment of the market. At the same time, COPPA gives both federal and State governments an important enforcement tool to ensure that website operators meet the minimum standards established by Congress.

II. §312.2 DEFINITIONS

A. Disclosure

We recommend that the Commission specify that contractors who provide technical support or fulfillment services will be exempted from the definition of "disclosure" only if (1) the contractor does not use or maintain any information about the child beyond that which is necessary to perform its technical support or fulfillment services, and (2) the contractor deletes that information as soon as its retention is no longer necessary. Moreover, the tasks necessary to perform technical support or fulfillment services should be explicitly defined to exclude transfers to third parties. The Commission should also clarify that clauses (a) and (b) in the definition of "disclosure" set forth two different means of disclosure, perhaps by replacing the word "and" between these clauses with the word "or."

B. Operator

The proposed Rule does not treat an affiliate as an "operator" based on its corporate relationship to an operator, but instead looks to the manner in which the affiliate itself uses data. The issue of sharing of information among corporate affiliates was hotly debated during legislative discussions regarding recent amendments to the federal Fair Credit Reporting Act ("FCRA"). Over the objections of various states, the FCRA was amended to exempt from its coverage information shared among corporate affiliates. See 15 U.S.C. § 1681a(d)(2)(A)(ii), (iii). Recent reports of alleged abuses of this exclusion in the credit reporting arena give rise to concerns about the creation of a similarly broad exclusion in the area of children's online privacy. At the appropriate time, but no later than the Commission's review of COPPA's implementation pursuant to §1307 of the Act, the Commission should examine the transfer of data from operators to affiliates. If such sharing is sufficiently pervasive, the Commission should consider whether to define "operator" in a manner which includes corporate affiliates.

C. Verifiable Consent

The inclusion of the phrase "available technology" in the definition of "verifiable consent" appears to be designed to provide operators with maximum flexibility in determining how best to use technology in their efforts to comply with both the notice and consent requirements. We recommend that the proposed Rule be clarified to ensure that under no circumstances could a limitation in available technology which makes it difficult to provide notice or obtain consent be interpreted to excuse an operator from obtaining the required consent.

D. Website or Online Service Directed to Children

As the proposed Rule states, an operator of a general interest website or online service is covered by the proposed Rule if it knows that a particular visitor is a child under the age of 13. The Commission should consider whether the term "knowledge," as used here and in §312.3, should be defined to include both actual knowledge and instances where it would be reasonable for the operator to infer that the visitor is under the age of 13. Specifically, the Commission should consider whether operators who receive information indicating that the website visitor is 18 or under should be on notice regarding the possibility that the visitor may be under 13 as well. Such operators should be required to further inquire whether a visitor who reports that he or she is under the age of 18 is in fact under the age of 13. Otherwise, general interest websites could avoid any obligation to comply with the Act by creating an age classification question that includes both teenagers and children in the youngest age category (*e.g.*, by creating a "15 and under" category).

III. §312.4 NOTICE TO PARENTS

A. §312.4(a) General Principles of Notice

We believe that the Commission has set forth an effective standard for requiring prominent links to a website's information practice disclosures.

B. §312.4(b)(2)(i) Notice by Multiple Operators

The Commission should consider requiring multiple operators who provide notice pursuant to §312.4(b)(2)(i) to agree upon a single policy with respect to children's information. Alternatively, as footnote 9 of the proposed Rule suggests, multiple operators should have joint responsibility for furnishing a single notice explaining their policies in a format that is both comprehensive and simple, including contact information for each operator. Multiple operators should also designate one

operator as the principal point of contact for parents who have questions about the use of their children's data. While all operators would be equally responsible for the accuracy of the information provided to parents, such an arrangement would ease the burden on parents and minimize the likelihood that they will be provided with inconsistent responses to their questions.

C. §312.4(b)(2)(iv) Disclosures Regarding Third Party Practices

The proposed Rule requires website operators to obtain parental consent prior to any transfer of information collected from children to third parties. The Commission should consider whether, when providing notice pursuant to §312.4(b) and (c), operators should be required to specifically notify parents about any material differences between the information practices of the operator and those of the third party. Such information would be more meaningful than a general statement as to whether the third party has agreed to maintain the confidentiality, security, and integrity of the personal information it obtains from the operator, as is currently required by the proposed Rule.

As enacted, COPPA places primary responsibility for controlling information collection and use on website operators, rather than on third parties obtaining such information through transfer. We recommend that at the appropriate time, but no later than the Commission's review of COPPA's implementation pursuant to §1307 of the Act, the Commission should revisit this scheme, to determine whether the statute and its implementing regulations provide for adequate control of the manner in which data is used by a third party transferee, and report any deficiencies in this regard to Congress.

D. §312.4(b)(2)(vi) Parental Option to Review, Change, or Delete Data

Under the proposed Rule, a parent has the right to review personal information provided by his or her child and to make changes to and/or have that information deleted. The Commission has

inquired about the appropriate method for notifying parents of this right. We recommend that the Commission retain the requirement set forth in the proposed Rule that this information be posted on the operator's website or online service, as well as being provided directly to parents. Ongoing access to this information will remind parents of their continued right to request review, alteration, or deletion of their children's data.

As noted above, COPPA and the Commission's proposed implementing regulations raise questions about the use of information by third parties which should be revisited in the future. Specifically, the Commission should consider whether a parental request to delete data should also apply to require deletion of data that has been transferred to a third party.

E. §312.4(c) Methods for Providing Notice

We favor providing operators with the flexibility to determine how best to convey notice to parents given the technology available at that time. However, as stated previously, we believe that limitations in the available technology should not excuse an operator from obtaining the consent required in §312.5.

F. §312.4(c)(1) Content of the Notice to the Parent

The States believe that all of the elements for required notice to parents set forth in §312.4(c)(1) are important to informed parental decision-making. Parents need detailed information about how their children's data will be used and disseminated prior to granting consent. They also must be clearly informed of their rights to limit the use and dissemination of the information. To ensure that these goals are met, it might be advisable to require operators to inform parents of what specific steps must be taken to convey a request to prohibit further contact with a child or require

deletion of a child's data. The Commission might also require that notice to parents specify what rights to redress are available if the operator violates its declared information practices policy.

IV. §312.5 General Requirements for Parental Consent

Section 312.5 requires an operator to send a new notice and request for consent to parents when the operator wishes to use the information in a manner not covered by the original notice. Such circumstances might include a situation where the operator wishes to make disclosure to a party not included in the original consent. Under the proposed Rule, the circumstances triggering this requirement would include the creation of a new corporate entity, by either a merger or other corporate combination involving the existing operator or a third party. This interpretation of the Act is a reasonable means of ensuring that a corporate merger or acquisition does not render parental consent meaningless.

It is also worth noting that the Commentary to §312.5 of the proposed Rule states that an operator must obtain verifiable consent prior to using or disclosing any information already in its possession, as of the effective date of the proposed Rule. We commend the Commission for its proactive stance on this issue, which we believe is consistent with Congress' goals in enacting COPPA. However, if the Commission were persuaded, based on comments submitted by operators, to eliminate the protection afforded to the use or disclosure of previously collected information, the Rule should at a minimum apply to the use or disclosure of information collected on or after the date that COPPA was duly signed into law.

A. §312.5(b) Mechanisms for Verifiable Parental Consent

Section 312.5(b) sets forth the standards for assessing whether a particular mechanism for obtaining parental consent would be deemed in compliance with the proposed Rule. The

Commentary to this section suggests that a simple e-mail message from the parent's account, unaccompanied by some sort of digital signature, would not be considered verifiable parental consent.

We agree that children could easily circumvent e-mail consent methods that do not utilize digital signatures or other similar verification mechanisms. Children often share a parent's e-mail address and can easily intercept, even inadvertently, requests for parental consent. Alternatively, if a child has her own e-mail account, the child could redirect requests for consent to that account, by supplying her e-mail address instead of her parent's.

While forcing operators to resort to methods of obtaining consent other than by ordinary e-mail may create additional costs for online marketers, it is likely that such effects will last only until digital signatures and other verifiable electronic mechanisms come into common use. In the interim, we agree with the Commission's assessment that the e-mail-based systems currently used by many websites are not verifiable and do not satisfy the Congressional mandate set forth in the Act. We join the Commission in inviting industry to develop consent mechanisms that would permit parents to accept or reject an operator's request quickly and easily, while minimizing the possibility that a child could readily forge parental consent.

B. §312.5(c) Exceptions to Prior Parental Consent

Section 312.5 sets forth a number of exceptions where either notice and/or consent would not be required under the Act. While these exceptions generally appear reasonable, we recommend that the proposed Rule clarify that these exceptions should be construed narrowly so as to minimize their potential for circumventing the Act's restrictions. This is particularly true of the first three exceptions enumerated in Section 312.5, which deal with special circumstances where data collected from children will be used without parental consent for certain limited purposes, such as contacting parents

to obtain consent or responding to discrete inquiries from children. Along these lines, the Commission should consider explicitly noting that these exceptions may not be used to justify transfers to third parties--other than law enforcement officials investigating matters concerning public safety.

V. §312.8 Confidentiality, Security, and Integrity of Personal Information Collected from Children

Section 312.8 requires operators to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. We agree with the Commission's conclusion that data security is a vital goal, and believe that operators should be given a good deal of flexibility in determining how best to comply with this requirement. At a minimum, however, we recommend the following:

1. that operators use only secure webservers when collecting information from children;
2. that information be placed behind firewalls where doing so would be appropriate;
3. that information be retained in retrievable form only as long as necessary;
4. that information is deleted as soon as it is no longer being used; and
5. that only employees who are authorized to access data be permitted to do so.

VI. CONCLUSION

We wish to thank the Federal Trade Commission for the opportunity to comment on its proposed Children's Online Privacy Protection Rule. Moreover, we commend your efforts to protect our children and support final adoption of the Commission's proposed Rule. Without the protections contained in the proposed Rule, threats to the privacy of our children from online marketers are likely

to increase and undermine the enormous educational and civic opportunities promised by the Internet. We also recognize that the issues underlying the proposed Rule are difficult ones, particularly because of the quickly-changing nature of e-commerce and the Internet itself. We believe that the Commission's Rule is sensitive to these difficulties, and that it will meaningfully ease the anxieties of parents, clarify the responsibilities of industry, and enable both the Commission and the State Attorneys General to ensure that the standards set forth in the Act are met. Finally, we look forward to actively participating in the Workshop that will address these questions in greater detail.

Sincerely,

ELIOT SPITZER
New York Attorney General

Caitlin J. Halligan
Chief, Internet Bureau

BILL PRYOR
Alabama Attorney General
Dennis Wright
Assistant Attorney General

JANET NAPOLITANO
Arizona Attorney General
Sydney K. Davis
Assistant Attorney General

BILL LOCKYER
California Attorney General
Herschel T. Elkins
Senior Assistant Attorney General

ROBERT A. BUTTERWORTH
Florida Attorney General
Jack A. Norris, Jr.
Chief, Multi-State Litigation

BARRY W. REID
Administrator, Georgia's Fair Business Practices Act, and
Governor's Office of Consumer Affairs
John S. Smith, III
Counsel and Division Director

JO ANN UCHIDA
Executive Director
State of Hawaii Office of Consumer Protection
Stephen H. Levins
Supervising Attorney

JIM RYAN
Illinois Attorney General
Deborah Hagan
Kathleen Dravillas
Assistant Attorneys General

JEFFREY A. MODISETT
Indiana Attorney General
Lisa R. Hayes
Chief Counsel, Division of Consumer Services

CARLA J. STOVALL
Kansas Attorney General
C. Steven Rarrick
Deputy Attorney General

J. JOSEPH CURRAN JR.
Maryland Attorney General
William D. Gruhn
Assistant Attorney General

FRANKIE SUE DEL PAPA
Nevada Attorney General
Grenville T. Pridham
Deputy Attorney General

BETTY D. MONTGOMERY
Ohio Attorney General
Helen Mac Murray
Chief, Consumer Protection

W.A. DREW EDMONDSON
Oklahoma Attorney General
Jane F. Wheeler
Assistant Attorney General
Director, Consumer Protection Unit

PAUL SUMMERS
Tennessee Attorney General
Timothy Phillips
Assistant Attorney General

WILLIAM H. SORRELL
Vermont Attorney General
Julie Brill
Assistant Attorney General

CHRISTINE O. GREGOIRE
Washington Attorney General
David M. Horn
Assistant Attorney General