WILMER, CUTLER & PICKERING

e-commerce news

October 29, 1999

New Developments: Children's Online Privacy Regulations

New regulations under the Children's Online Privacy Protection Act of 1998 provide for broad control by parents of the process by which children's personal information is gathered. These regulations place limits on the collection, use and disclosure of such information by both commercial web sites that are directed at children and commercial sites that are not directed at children but whose operators know that the information they are collecting is from a child. If your company web site gathers personal information from anyone (including through cookies or other passive means), you should be aware of the details of these new regulations.

ACTION ITEMS:

- All web sites directed at children (or sites that know that information they are collecting is from a child), will need to place a notice on the site that tells visitors:
  * what personal information it collects from children;
  * how the information is used, and;
  * whether the information is disclosed to third parties.

- In general, web sites should obtain **parental consent** for any collection, use, or disclosure of personal information about a child *before* it collects that information. In obtaining consent, web site operators may utilize a variety of means to confirm parents' identity, such as the use of credit card numbers or digital signatures.

Background. On October 21, the Federal Trade Commission issued its final rules under the Children's Online Privacy Protection Act of 1998 ("the Act"), detailing the manner in which web sites may collect and use "personal information" from children. The rules go into effect on April 21, 2000, after which web site operators who fail to bring their sites into compliance risk civil penalties, including fines of up to $11,000 per infraction.

The rules are aimed primarily at web sites designed for children under age 13, but they also apply to general-audience web sites to the extent the operator of the site has "actual knowledge" that it is dealing with a child's personal information. In general, the rules require that web site operators obtain prior verified parental consent before collecting any personal information from a child under 13. There are narrow exceptions to the parental consent requirement, such as the right to respond to a one-time e-mail from a child; these exceptions are most relevant to sites that are not aimed specifically at children. Sites that are directed to children must prominently post a detailed policy statement on the site. Web sites that merely provide access to the Internet, without collecting information, are not covered by the rules. The highlights of the rules are set forth below.

Collecting "Personal Information." The Act applies to the online "collection" of "personal information." Collection occurs any time an

operator finds itself in possession of information - this could happen, for example, when a web site passively receives a child's e-mail. Tracking, through cookies and other technology, is also considered collecting. Allowing online posting (unless personal information is stripped from the postings) is considered collection as well. "Personal information" is similarly broadly defined to include a child's name, home or e-mail address, phone number, social security number, photograph coupled with an identifier, or any other persistent identifier such as a processor's serial number that could be stored in a cookie or other tracking device. Any information that is linked with an identifier also would be covered.

Obtaining Verified Parental Consent. The FTC struggled with the Act's requirement that prior parental consent be obtained before personal information is collected from a child by a web site. Verification of such consent presents technological and financial challenges for web site operators. The costs of obtaining verified consent are likely to present a burden for start-up, independent sites. Another issue raised by the consent requirement is the hurdle it may pose for children whose parents are not computer literate, do not own a computer, or are non-English-speakers. Consent also raises unique issues with respect to use of the Internet in school settings (where parents or other legal guardians are not present). Nonetheless, the FTC appears to have effectively balanced these competing interests in its initial attempt to craft reasonable rules, and it will revisit the question in October 2001. For now, the rules establish a so-called "sliding scale" approach to verified consent:

- For uses of personal information that are "internal" to the site or its operation (for example, information used to provide services to the child), the rules permit operators to rely on a parent's e-mail consent to the gathering of personal information, provided the operator follows up with a confirming e-mail or letter.

- For any uses of personal information involving disclosure to third parties – which are defined to include allowing a child to post information online – the rules require more secure methods of verification. These include having the parent send in a consent by letter or fax, use of a credit card in conjunction with online consent, use of a PIN or password, toll free calls to trained personnel, digital certificates, or similar measures.

Exceptions to the Prior Consent Requirement. The rules provide four exceptions to the prior parental consent requirement. These exceptions are to be narrowly construed, and apply *only* to the collection (and use) of a child's *online contact information*. A site is permitted to collect and use such information in the following circumstances:

- To seek parental consent or provide parental notice. If an operator has not obtained the requested consent after a reasonable period of time has passed, the information must be deleted. Note that this exception allows collection of the parent's name and e-mail address as well. Interestingly, while the consent rules envision the possibility of sending a letter to the parent's home, this exception does not permit collection of a home address without prior consent. Thus, in practice, a home address generally should be collected directly from the parent unless the parent has already given consent, through other means, to its collection from the child.

- To respond once to a request from a child, provided that the operator may not use the information for any other purpose, including any other contact with the child, and must delete the information immediately after responding to the child's request. This exception is designed to allow general-audience sites to respond to an unsolicited e-mail from a child (assuming, of course, that the site has "actual knowledge" that the e-mail is from a child).

- To respond on a repeated basis to a request from a child — for example, where a child requests an online subscription or signs up for regular homework assistance. The FTC suggests that entry into a contest in which an award later will be given would be covered by this exception, but because the exception applies only to "online contact" information, this example may not have broad implications. To qualify for this exception, the operator may not use the child's information to contact the child beyond the scope of the request, and, after the initial use of the child's information in order to respond to the child's request, the operator must make a "reasonable effort" to provide the parent with notice and an opportunity to "opt-out." The notice to the parent may be sent by e-mail, and it must describe the

purpose of the collection of the information as well as the parent's right to prohibit further use of the information and contact with the child and to demand deletion of the information. The notice also must explain that if the parent fails to respond, the operator may use the information in the manner described.

- To protect the safety of a child using the site. Such information cannot be used, however, to re-contact the child or for any other purpose, and notice must be provided to the parent as described above.

- To protect the security or integrity of the site, to protect against liability, to respond to judicial process and other legal inquiries, but only to the extent "reasonably necessary."

Posting of a Privacy Notice. The rules require that any site or service aimed at children "prominently" post a privacy statement that clearly articulates the site's collection practices with respect to children's information. The notice must be posted on the home page and at every area where personal information is collected from children. The notice (as well as the individual parental notice under the consent exceptions) must contain the following information:

- The name, address, telephone number, and e-mail address of the site's operator (an "operator" may include any entity on behalf of which the site collects information, such as a sponsor).

- The types of personal information the site collects from children and how it is collected (directly or passively, for example).

- How the operator will use the information, including any disclosure to third parties, in which case such parties must be generally identified and their use of the information must be explained as well; any assurances such parties have provided regarding the security and confidentiality of the data must be explained. Parents must be informed that they may refuse to permit such third party disclosure.
- A reassurance that the operator will not condition a child's participation in any game or activity on the provision of more personal information than is necessary to participate.

- Information concerning how parents can review and delete their child's personal information from the web site's database and refuse to permit further collection or use of their child's information.

Permitting Parental Access to Information. The new rules require that web sites give parents the opportunity to review and delete personal information collected from their child. Although web sites do not have to provide parents with the ability to update or alter their child's information, the FTC recommends including such an option, and other privacy regulations (such as the EU Directive) require it.

Before providing parents with access to the child's information, however, the operator must verify that the requesting party is, in fact, the parent. The acceptable methods of verification mirror those that may be used to obtain parental consent for third party disclosure.

Obtaining New Consent. Web site operators must provide new notices to parents when there has been a material change in the way the operator collects, uses, and/or discloses the child's personal information. For example, if a child has been granted parental consent to provide information necessary to play games at a particular site, but the child seeks to participate in a chat room where identifying information is not stripped, parents must be notified and new parental consent received. In addition, if a web site owner merges with another company and wishes to use a child's personal information to market materially different products or services, it must also notify the parents and receive new parental consent.

Safe Harbor Protection. A web site's compliance with FTC-approved self-regulatory guidelines qualifies that web site for safe harbor protection in any enforcement action for violations of the Act. Seal programs (such as bbbOnline and TrustE) will no doubt seek to obtain such approval for their guidelines.

Lynn R. Charytan, lcharytan@wilmer.com
202/663-6455
Laura L. Kotanchik, lkotanchik@wilmer.com
202/663-6273

Cybersquatting. On Oct. 26, the House passed legislation (S. 1255) that would prohibit cybersquatting, the practice of registering an Internet domain name or web site containing a proprietary title with the intent of selling it to the trademark's owner for a profit. The measure would establish civil damages of up to $100,000 for each unsolicited use of a proprietary name as a domain name. Before approving the measure, the House voted to insert the language of its version (H.R. 3028) into the Senate-passed bill. (See September 1999 issue of ECommerce News.) The Administration has expressed concerns over the legislation as passed and is considering a veto.

Electronic signatures. Next week, the House is expected to consider legislation (H.R. 1714) to promote electronic commerce and establish a single nationwide standard for the use and recognition of electronic signatures. Approved by the Judiciary committee on Oct. 13 and the Commerce Committee last month, H.R. 1714 would prohibit companies from refusing to honor electronic signatures on business contracts or transactions. Since the Commerce and Judiciary Committee passed separate versions of the bill, members must work to iron out a compromise.

The bill is expected to reach the floor with an amendment offered by Rep. Tom Bliley (R-VA) that may attempt to address some of the Democratic concerns about preempting state law and retaining records from electronic transactions. Republican leaders are hoping that Bliley's amendment will be enough to garner the two-thirds majority necessary to pass the legislation.

Financial privacy. House and Senate conferees are expected to file their conference report on financial services legislation (S. 900) this week. As soon as the report is filed, the House and Senate are expected to act quickly on adopting the compromise. S. 900 would repeal the Glass-Steagall law and amend the 1956 *Bank Holding Company Act* to allow banks, brokerages and insurance companies to enter one another's businesses. Under the measure, financial institutions would be required to disclose their policies annually and allow customers to "opt out" of having their information shared with unaffiliated third parties. However, information could be shared among a corporation's affiliates or in joint marketing agreements between banks and other financial institutions.

SPAM. Two new pieces of anti-spam legislation were introduced this month. Most recently, on Oct. 21, Rep. Heather Wilson (R-NM) introduced H.R. 3113, a bill to protect individuals, families, and ISPs from unsolicited and unwanted electronic mail. And, on Oct. 5, Rep. Chris Smith (R-NJ) introduced H.R. 3024, a bill to restrict the transmission of unsolicited electronic mail messages.