

Age Verification of Children

The California State PTA has long been interested in Internet safety, especially as it applies to children.

Age verification is a concept that has been under consideration recently by many Internet experts to see if it can be a helpful electronic way to protect children from exposure to inappropriate Internet content and from the wrong kinds of interactions with strangers online. The concept has also spawned entrepreneurial businesses.

In this brave new rapidly changing world of cyberspace, there are many important reasons why parents need to proceed carefully and cautiously.

California State PTA has been researching the process of age verification, and the burgeoning marketplace of commercial age verification businesses, so we can help all parents be informed.

Commercial Age Verification

Commercial age verification businesses advertise a service to protect children from inappropriate Internet content, and from interactions with unknown individuals who claim to be children of a certain age, but who may, in fact, be a different age. In a typical service, a parent pays a registration fee and fills out a form giving the child's name, address, age, school, email address, etc. Then the child's school is asked to verify the information parents provide when they register a child. A school secretary, the PTA president, or some other source within the school is usually asked to do the verification.

The age verification business then enters the verified information into its database, and by electronic means, activates certain controls to limit Internet interactions by the child.

Age verification companies may also offer PTAs and schools fund-raising opportunities, in which all or part of the registration fee is shared with the PTA or the school, especially in exchange for the school providing the verification.

Consider Safety and Security

In considering whether an age verification service should be utilized, parents should consider issues such as the safety and security of students' information. For instance, when a parent registers a child with an age verification service, all or part of the child's registration information may be sold to partnering web-sites that create marketing profiles of their users.



No Substitute for Direct Parent Monitoring

Internet experts and purveyors of age verification services agree that there is no substitute for direct parent monitoring to safeguard children online. But it must be emphasized that any time a business seeks information about you, or especially about your child, it is critical that you know exactly why the information is needed, how it will be used, and how it will be safeguarded. Because we know that the information has commercial value to businesses, it is reasonable and appropriate to ask any business exactly how it plans to use any information collected to earn a profit.

Special Study Group

In January of 2008 a special study group was formed by MySpace and 50 State Attorneys General to study ways in which technology can help to safeguard child Internet users. The group called for the creation of an Internet Safety Technical Task Force, which met for a year, hosted by Harvard University's Berkman Center for Internet and Society. In December of 2008 the group's final report was issued. In that report, the Task Force had this to say about age verification:

"Age verification and identity authentication technologies are appealing in concept but challenged in terms of effectiveness. Any system that relies on remote verification of information has potential for inaccuracies. For example, on the user side, it is never certain that the person attempting to verify an identity is using their own actual identity or someone else's. Any system that relies on public records has a better likelihood of accurately verifying an adult than a minor due to extant records. Any system that

"Any central repository of this type of personal information would raise significant privacy and security issues."

focuses on third-party in-person verification would require significant political backing and social acceptance. Additionally, any central repository of this type of personal information would raise significant privacy and security issues."

Parents need to consider all of this before they decide to give anyone information about their child.

