



February 25, 2008

The Honorable Tom Cross
316 Capitol Building
Springfield, IL 62706

RE: HB 4874 Social Networking Website Access Restriction Act

Dear Minority Leader Cross:

On behalf of the high-tech industry, AeA (American Electronics Association) would like to express our concerns with HB 4874, “Social Networking Website Access Restriction Act.” AeA is dedicated to the online safety of children and work with companies to develop tools and standards of online behavior to in fact keep children safe. Therefore, it is AeA’s belief that despite this bill’s good intentions to protect Illinois children it will actually increase the very risks it is designed to combat. Consequently, AeA opposes the passage of HB 4874 because it will in fact increase the risk to children.

Age Verification/ Parental Consent

Inherent in the legislative language of HB 4874 is the idea of the “social networking website” being able to verify the ages of all the customers who use the site. Under threat of criminal penalty, websites would be required to identify with certainty that a parent has given minors consent to use a social networking website. Also, the website would need to authenticate that the party providing parental consent is, in fact, the parent. AeA believes there are several problems with this approach.

To date there is no proven mechanism for age verification for users under the age of 18. A report conducted on December 20, 2006, by the Virginia Attorney General Youth Internet Safety Taskforce¹ came to this conclusion. Finding a dependable source of verification credential for a minor or an adult and then matching it to someone sitting at the other end of the computer is a difficult task in and of itself. Of course, this is of particular concern in the case of a minor, due to the lack of available credentials or certificates that can verify a minor. In fact, as a high-tech trade association, we have yet to see an age verification tool or system that is reliable. Even under the most ambitious proposed concepts 100% certainty, sufficient to protect against criminal liability, is not possible. In reality, under present technological and public policy conditions, age verification technology is a mirage and not a panacea to rid the Internet of harm to children.

Theoretically, there are basically two approaches to age verification: 1) a legitimate party, e.g., a driver’s license bureau, makes identity claims on behalf of a particular person which an online service can use to verify age or 2) a person provides the website with a real name and address, which are then checked against various databases (e.g., credit bureaus, social security database,

¹ See, e.g., <http://www.vaag.com/InternetTaskForce/ReportYISTFfinal.pdf>

etc.). Both scenarios raise significant privacy and security issues, including legal issues that have not yet been addressed.

Moreover, it is not yet clear that implementing either approach will increase child safety. From a recent report on online safety:

Age verification, on its own, doesn't indicate whether or not a person is a convicted sex offender. Mandated age verification, as proposed, would allow the hundreds of thousands of offenders... who are over 18, unrestricted access to sites. Worse, it would allow these offenders the ability to vouch for children that might or might not exist. This is where it gets most dangerous. People might assume that "verified" users have undergone some type of vetting, and let their guard down just that little bit the offenders need to exploit. In the case of convicted sex offenders, age verification actually helps them by giving them an additional layer of legitimacy.²

Thus, age verification could have a negative side effect of making children less safe online, due to the scenario described above of a convicted sex offender creating a profile that depicts a sex offender as a minor.

Enforcement of HB 4874

Furthermore, one must question whether Illinois could enforce this law against such services. HB 4874 raises legal concerns because it is trying to accomplish by statute what is already barred by federal law. First, the Communication Decency Act of 1996 (CDA)³ would almost certainly prohibit any enforcement by state attorney generals. Numerous federal courts effectively have interpreted §230(c)(1) to mean that no state law can impose liability on a service provider for failing to protect the public from the words, acts, or communications of third parties. Allowing states, like Illinois, to implement and enforce such statutes would subvert the intended effect of the CDA's immunity provision and expressly make online service providers liable when the harm sought to be avoided is created by "another information content provider."

Second, HB 4874 would likely violate the U.S. Constitution's Supremacy Clause, which requires that the CDA's protections, not state law, prevail. As the Supreme Court reasoned in *Gonzales v. Raich* (overturning California's "medical marijuana" laws),⁴

"the supremacy clause unambiguously provides that if there is any conflict between federal and state law, federal law shall prevail. It is beyond peradventure that federal power over commerce is 'superior to that of the States to provide for the welfare or necessities of their inhabitants, however legitimate or dire those necessities may be.'"⁵

² See Adam Thierer, "Social Networking and Age Verification: Many Hard Questions; No Easy Solutions." *The Progress & Freedom Foundation*, March 2007, <http://www.pff.org/issues-pubs/pops/pop14.5ageverification.pdf>

³ 47 U.S.C §230

⁴ *Gonzales v. Raich*, 545 U.S. 1, 29 (2005).

⁵ *Id.*

Additionally, HB 4874 may violate U.S. Constitution's Commerce Clause. Under *American Libraries Association v. Pataki*,⁶ which struck down a New York Internet obscenity law, state laws governing the Internet violate the Commerce Clause if websites cannot feasibly isolate and restrict communications to those states' residents. This avoids effectively giving one state's law extraterritorial effect.⁷

Other Solutions

Despite the technological and legislative obstacles to age verification, there are avenues in which state officials and the high-tech community can work hand in hand to protect Illinois children. Online safety requires a multi-faceted approach involving ever evolving technology, public education, and partnerships with law enforcement and other groups to keep the Internet safe for children. There are already technical solutions in place that help parents and children make sure their experiences on the Internet are safe and fun. For example, parental controls allow parents to manage exactly what their children do on their computers, from what games they can play to which programs they can use, and which websites they can visit. Moreover, parents can set age-appropriate limits for each child in the family.

In addition to the many tools and processes that companies and non-governmental organizations already have in place to help address this issue, there are other steps that should be taken to increase child online safety. In general, we recommend a) providing new and more effective tools for law enforcement; b) increasing penalties for child predators; and c) creating new innovative ways to increase the awareness of parents and children to the dangers that currently exist online.

Law Enforcement

We applaud Illinois on focusing on the intervening criminal acts that place children in danger with the introduction of HB 4875, HB 4876, HB 4877, HB 4878, and HB 4879. In particular, HB 4875, "The Sex Offender Registration Act," imposes certain conditions of parole on anyone convicted of certain sexual crimes involving a minor. These conditions include:

- (1) continued supervision of the person's incoming and outgoing email or any other Internet-based communication by a probation officer, parole office, law enforcement officer or assigned computer information technology specialist in a manner and form prescribed by the Attorney General;
- (2) period unannounced examinations of the person's computer or any other device with Internet access, including the retrieval and copying of all data from the computer or device and any internal or external peripherals and removal of such information, equipment or device to conduct a more thorough inspection.

Furthermore, HB 4876, HB 4877, HB 4878, and HB 4879 would amend and codify the crimes of possession of child pornography and the solicitation of a child by the knowing use of a computer on-line service. By shifting the focus on the criminal actors, Illinois is better served in protecting children, than implementing an age verification system that is a mere mirage.

⁶ *American Libraries Association v. Pataki*, 969 F. Supp. 160 (S.D.N.Y 1997).

⁷ *Id* at 182.

Education

One of the most effective ways to ensure that children do not become victims of cyber crimes is to make sure every school teaches its children a minimum set of prevention methods in all areas of cyber awareness. We congratulate Illinois taking the lead last August and passing Public Act 095-0509, which requires schools to teach online safety as part of their school curriculum. Creating school internet safety policies will help children recognize, respond to, and report dangerous situations they may come across while online. In the past, schools have led the charge to educate our youth on ways to protect themselves from threats they may come across in their neighborhood, like “don’t talk to strangers” or “just say no.” Once again, schools must take the lead to educate our children. In an age where students are being encouraged to use the Internet for education purposes, learning how to properly, safely, and securely use the Internet is critical if students are to reap its benefits.

Conclusion

Once again, I wish to reiterate AeA and its member companies’ dedication to online child safety. We are willing to work hand in hand with Illinois to ensure the safety of children and find ways to combat online threats to children. AeA is the nation's largest high-tech trade association and represents over 1.8 million high-tech workers in more than 2,500 IT sector companies which span the high-technology spectrum, from software, semiconductors, medical devices and computers to Internet technology, advanced electronics and telecommunications systems and services. Complete information on AeA and its mission is available on our website at www.aeanet.org.

We thank you again for your work on this issue and look forward to continuing to work with you on this important legislation. Should you have any questions, please do not hesitate to reach me at 630-613-7174 or you can reach our Manager and Counsel of Public Policy, Alan Vazquez, in our Washington, DC office, at 202-682-4439. Thank you.

Sincerely,

A handwritten signature in black ink that reads "Ed Longanecker". The signature is written in a cursive, flowing style.

Ed Longanecker
Executive Director
AeA Midwest Council