

# Digital Identification and Schools

Nancy Willard, M/S., J.D.  
Center for Safe and Responsible Internet Use  
November 2008

This nation's Attorneys General have been promoting the idea of using digital identification (also called age verification) ostensibly to protect young people from online predators.<sup>1</sup> While protecting young people is indeed a very worthy objective, the push for a technology "quick fix" to this concern appears to have some very undesirable unintended consequences. Two companies are now seeking the assistance of schools to digitally identify students. Both companies are planning to provide demographic information about students to web sites to enable those sites to engage in more effective targeted advertising to these young people. This additional use of student demographic data has not been fully disclosed to school or parents.

## Youth Risk Online

Most of what people think they know about online sexual predators is wrong. An excellent article by the Crimes Against Children Research Center outlines the myth and realities.<sup>2</sup> Online sexual predation cases are very rare. Young people face far greater risks of sexual abuse from family members and acquaintances, who might now be using technologies for grooming. Predators are not targeting children. They seduce teens by talking about sex - which would lead to a "yuck" response from a child. They are not deceiving teens about their age or sexual intentions - but may pretend that they are in love with the teen. They are not tracking and abducting teens based on personal information they post online. They entice vulnerable or "seeking" teens to meet with them. The teens who are at greatest risk of sexual predation are those who are already "at risk." Predators target teens who post sexy pictures, use sexy usernames, and visit chat rooms where people discuss sex.

Research has documented that the teens who are at the greatest risk online - engaging in risky sexual activities, cyberbullying, and involvement with unsafe online communities or dangerous groups - are the ones who already at greater risk in the real world.<sup>3</sup> Further, the teens face greater risks from known peers - other teens. However, it is also important to note that the majority of young people are generally making good choices online and effectively responding to the negative incidents that occur.

## Digital Identification of Minors

Digital identification is a technology that holds promise for some uses. Using credit cards, it is possible to prevent minors from accessing adult sites. Using driver's license data, it will soon be possible for adults to establish identification that will allow for more secure financial transactions. But in order to establish a digital identification, it is necessary to have a government or business entity verify the identity and age of the user. Easy to do for adults.

Who has this information for minors? Schools.

### **EGuardian and Identity.net**

Apparently without any analysis of the concerns related to using schools to verify the identity, age, and custodial authority of an adult over a student, two companies are already “knocking on the doors” of schools asking for their assistance in digitally identifying students. EGuardian, which is apparently targeting elementary and middle schools, has partnered with WoogiWorld and Identity.net, which has targeted middle and high schools, has partnered with I-Safe.<sup>4</sup>

What these companies are not telling schools or parents is that their business model involves transferring demographic data - age, gender, and location, as well as other information - to web sites so that web sites can more effectively advertise to young people. This is called targeted advertising. Because targeted advertising is known to be more effective in influencing young people to “nag” their parents to purchase products or services, the sites can charge more for the advertisements, and the digital identification company receives a portion of this increased advertising income. With a digital identification, a user has a “unique persistent identifier” which could be used to track users across partner sites to determine their interests.

EGuardian promises that the digital identification will protect children. Their site starts with a fear message: “Every time your child goes online, he or she is exposed to predators, adult content and inappropriate sites.” There are very helpful desktop protections that are coming on the market that provide very effective way for parents to protect younger users while protecting their personal information, including Microsoft’s Vista Family Protections and Glubble.<sup>5</sup> EGuardian further encourages school involvement by providing a financial return. Parents pay \$29 to receive a digital identification for their child and EGuardian will refund \$11 to the school.<sup>6</sup> In an interview for the investment community, the founders noted their low cost of obtaining valuable information that can be sold over and over again to the sites for targeted advertising.<sup>7</sup>

The eGuardian application raises another concern. The application asks for the parent’s name, child’s name, address, and child’s birth date. What are the potential liabilities to a school if eGuardian’s security system fails and this information becomes available to others? If schools are to undertake this new activity which relates to student personal information there should be an entity that independently determine the sufficiency of the companies’ security systems. Schools should insist that the digital identification companies indemnify them for any misuse of student information.

I-Safe has created curriculum in partnership with Identity.net.<sup>8</sup> This curriculum makes no mention of the use of digital identification for targeted advertising, but does promote its use for safety from predators and cyberbullies. The teacher is provided with a notice to send home to parents asking for their permission to obtain a digital identification for their child. This notice also does not disclose the use of the identification for targeted advertising. There is a hint in the I-Safe curriculum that it is not even necessary to obtain parent permission. The materials state: “If necessary to comply with school

policies, send home Parent Permission Forms.” This raises the concern of disclosure of “directory information” to this company without any parent involvement.

Identity.net is advertising for partner sites.<sup>9</sup> It states: “The Identity.net Profile API allows partner sites to easily register users, automatically provide an OpenID for each user, and maintain a **rich profile of attributes about users**.” Translation: “extensive demographic data about students that will be used by the sites to target advertisements to them.” The site also provides a list of attributes that can be attached to the digital identification.<sup>10</sup>

### **Directory Information**

This new development raises issues related to school’s obligations under the Federal Rights and Privacy Act (FERPA) with respect to student director information.<sup>11</sup> This information includes: student’s name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. Schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Clearly, when the vast majority of parents receive notice about student directory information they are thinking use of their child’s contact information in school phonebooks or newsletters. In fact, under FERPA, this student information can be disclosed to many others - including commercial market profilers and advertisers.

Consider the outrage of parents if they were to find that these companies are coming to schools to obtain their children’s personal contact information. The key under FERPA is that while student directory information can be provided to others, there is no obligation to do so - except to military recruiters. It is highly probable that an amendment to FERPA is necessary to protect student and parent personal information in the digital age. Regardless of amendment, school districts can and should create policy to prevent the disclosure of student personal information to any commercial entity.

### **Privacy Policies**

Neither of the privacy policies of these two companies clearly disclose the use of demographic data for targeted advertising. Educators must understand how these sites manipulate the use of the term “personally identifying information” or “name and address.” EGuardian’s privacy policy states: “We will never disclose the name or address of any child or parent in our database to anyone.” While name and address information is helpful, it is not necessary for sites to engage in targeted advertising. The information the web sites want is age, gender, and geographic information - as well as interest information.

But if at any time on any site a user does provide a name and address, this can be added to the profile. Here is the tricky language Identity.net uses to explain this: “We will not disclose any of your personally identifiable information that you do not elect to make publicly available.”

The Identity.net privacy policy states that the site will not collect information from children under the age of 13. But the I-Safe curriculum is aimed for middle school students - the vast majority of whom are under the age of 13. The Children's Online Privacy Protection Act places significant restrictions on sites that obtain information from children under the age of 13.<sup>12</sup> Are there potential liabilities for schools that disclose student personal information to a web site that appears not to be in compliance with COPPA?

### **Targeted Advertising**

Why is targeted advertising so bad? Recently both the American Psychological Association and the American Academy of Pediatrics issued reports on the significant concerns associated with advertising to children and teens.<sup>13</sup> These concerns include psychosocial concerns around the values that advertisements are inculcating in our youth, the sexualization of youth, and increased parent-child conflict, as well as numerous health concerns, including obesity, poor nutrition, and use of violent media.

Given the documented harms caused by advertising, there is obviously no benefit to increasing the effectiveness of advertisers by providing them with greater demographic data to more precisely target young people. The web site Interactive Food and Beverage Marketing: Targeting Children and Youth in the Digital Age provides insight into this issue.<sup>14</sup>

### **Effectively Addressing Digital Citizenship and Youth Risk Online**

Schools must be at the forefront of addressing digital citizenship and youth risk online. While some refer to this issue as "Internet safety," the issues are more comprehensive. Given the degree to which interactive technologies are now pervasive in our society - and are now an important platform for business, political, community, and personal life, it is essential that schools prepare students to use these technologies safely and wisely.

We must ensure that young people gain the knowledge, skills, and values to independently make safe and responsible choices in a highly interactive, mobile technology environment where they are both consumers and creators of content and will interact with a wide range of people - and that effective comprehensive risk prevention approaches are implemented to address the concerns of the minority of young people who are at higher risk of being harmed or causing harm with these technologies.

All students must be supported to becoming good digital citizens. Digital citizens:

- Understand the risks. They know how to avoid getting in risky situations, detect if they are at risk, and respond effectively, including knowing when to ask for help.
- Engage in responsible, ethical behavior. Do not cause harm to others. Respect the privacy and property of others.
- Make sure their friends and others are safe. Report online concerns to an adult or the site.
- Promote online civility and respect.

As technology permeates instruction, the opportunities to address digital citizenship will increase. It must be understood that just as it is impossible for an adult to teach a young child how to swim without also getting into the water, schools must embrace these new interactive technologies or they will fail to effectively prepare students for their future.

Addressing youth risk online will require a more comprehensive effort. As noted, the students who are at greatest risk online are the ones who are already at greater risk. A collaborative effort of safe school and educational technology personnel will be necessary to develop research-grounded effective risk prevention initiatives to address the needs of these youth.

#### **About the Author**

Nancy Willard, M.S., J.D. is the director of the Center for Safe and Responsible Internet Use. She has degrees in special education and law. She taught "at risk" children, practiced computer law, and was an educational technology consultant before focusing her professional attention on issues of youth risk online and effective management of student Internet use. Nancy is author of two books. *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Cruelty, Threats, and Distress* (Research Press) and *Cyber-Safe Kids, Cyber-Savvy Teens, Helping Young People Use the Internet Safely and Responsibly* (Jossey Bass). Nancy's focus is on applying research insight into youth risk and effective research-based risk prevention approaches to these new concerns of youth risk online. She is working on professional development and parent/student resources to address digital citizenship and youth risk online.

Email: [nwillard@csriu.org](mailto:nwillard@csriu.org).

Website: <http://csriu.org>.

#### **Endnotes**

1 A task force has been established by the Berkman Center to investigate the use of digital identification to protect minors online. <http://cyber.law.harvard.edu/research/isttf>

2 Wolak, J., Finkelhor, D., Mitchell, K., and Ybarra, M. (2008) Online "Predators" and Their Victims: Myths, Realities, and Implications for Prevention and Treatment. *American Psychologist*, 63(2), 111-128. <http://www.unh.edu/ccrc/internet-crimes/>

3 Wolak, J., et. al. (2008), supra; Ybarra, M., Espelage, D.L., & Mitchell, K. (2007). The Co-Occurrence of Internet Harassment and Unwanted Sexual Solicitation Victimization and Perpetration: Associations with Psychosocial Indicators. *Journal of Adolescent Health*. 41(6,Suppl): S31-S41, S37; Rosen, L. D., et al., (2008) The association of parenting style and child age with parental limit setting and adolescent MySpace behavior, *Journal of Applied Developmental Psychology*, doi:10.1016/j.appdev.2008.07.005; <http://www.csudh.edu/psych/lrosen.htm>; McQuade, S. (2008) A Survey of Internet and At-risk Behaviors. Rochester Institute of Technology. <http://www.rrcsei.org/>. <http://www.rrcsei.org/>

4 <http://www.eguardian.com/> and <http://www.eguardian.com/>

5 <http://www.microsoft.com/windows/windows-vista/features/parental-controls.aspx> and <http://www.glubble.com/>.

6 <http://www.eguardian.com/teachers.php>

7 [http://www.thefrankpetersshow.com/podcasts/mp3\\_files/FP162-eGuardian.mp3](http://www.thefrankpetersshow.com/podcasts/mp3_files/FP162-eGuardian.mp3).

8 <http://www.identity.net/partners/isafe/curriculum/>.

9 <http://identity.net/profile/api/doc/index.php>

10 [http://identity.net/profile/api/doc/api\\_attributes.php](http://identity.net/profile/api/doc/api_attributes.php).

11 <http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>.

12 <http://www.ftc.gov/coppa/>.

13 Report of the APA Taskforce on Advertising and Children. (2004) [www.apa.org/releases/childrenads\\_summary.pdf](http://www.apa.org/releases/childrenads_summary.pdf); Policy Statement Children, Adolescents, and Advertising Committee on Communications PEDIATRICS Vol. 118 No. 6 December 2006, pp. 2563-2569 (doi:10.1542/peds.2006-2698) <http://pediatrics.aappublications.org/cgi/content/full/118/6/2563>; Report of the APA Taskforce on the Sexualization of Girls.(2007). [tp://www.apa.org/pi/wpo/sexualization.html](http://www.apa.org/pi/wpo/sexualization.html).

14 <http://www.digitalads.org/>