Why Age and Identity Verification Will Not Work - And is a Really Bad Idea

Nancy Willard, M.S., J.D.
Center for Safe and Responsible Internet Use
Website: http://csrui.org
Email: nwillard@csriu.org
January, 26, 2009

> "When we fall into the trap of believing or, more accurately, hoping that technology will solve all of our problems, we are actually abdicating the high touch of personal responsibility. ... In our minds at least, technology is always on the verge of liberating us from personal discipline and responsibility. Only it never does and never will. The more technology around us, the more the need for human touch."[1]

On January 14, 2008, the Berkman Internet Safety Technical Task Force issued its report, *Enhancing Child Safety and Online Technologies*.[2] The Task Force, a group of 29 leading Internet businesses, non-profit organizations, academics, and technology companies engaged in a year-long investigation of tools and technologies to create a safer environment on the Internet for youth. The Task Force was created in February 2008 in accordance with the Joint Statement on Key Principles of Social Networking Safety announced in January 2008 by the Attorneys General Multi-State Working Group on Social Networking and MySpace. This Task Force was formed as a result of pressure by some of the state attorneys generals upon the social networking sites to implement age verification technologies to separate adults from minors, ostensibly to protect minors from sexual predators.

The conclusion of the Berkman Task Force was:[3]

> 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 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 concerns and security issues.

Despite this very clear conclusion, Attorney General Blumenthal, who has been aggressively calling for age and identity verification for many years stated in response to this report:

> The report identifies 40 technologies that can make sites safer now, including age and identity verification tools. I am going to be working with other attorneys general to urge social networking sites to immediately begin implementing these technologies, especially age and identity verification.[4]

The Task Force Report outlined the concerns related to reliance on age and identify verification. The following points outline and add to these concerns:

- While it is possible to verify the age and identity of adults by using government issued records, like driver's licenses, or commercial records, like credit cards, there is no similar method that can be used to verify the identity of minors. Further whereas, the identity of an adult will remain stable over time, the identity of the adult(s) who have custodial authority over a specific minor can change.
  - Absent the creation of a RealID system that is initiated at birth, with constant upgrading of the data based on changes in custodial authority, it is not possible to accurately identify the age and identity of

---

[1] Naisbitt, J., Megatrends: Ten new directions transforming our lives, New York, N.Y. Warner Books, 1984.
[2] http://cyber.law.harvard.edu/pubrelease/isttf/
[3] Page 10.
[4] Steel, E. (January 13, 2009), The Case for Age Verification. *Wall Street Journal*. http://blogs.wsj.com/digits/2009/01/13/the-case-for-age-verification/.

minors. Without a secure way to achieve accurate identity information, any digital identification system could be easily corrupted.

- It has been proposed by some companies that schools could provide identification of minors.[5] This would place an additional workload on schools and lead to liability for mistakes. Microsoft has proposed that other community organizations, including churches, could also provide identification.[6] In addition to the concerns of liability, these organizations are places where sex offenders frequently create relationships with minors that result in sexual abuse. Search for "youth pastor sex abuse." Further, given the number of possible "schools" or "community organizations" this approach would lead to an easy process to create black market identifications.

  - There is no substitute for a RealID system for minors that would be secure and not raise other concerns.

- The Internet is global. The U.S. Congress has already attempted to require sites with adult material to use age verification through the Children's Online Protection Act. The effectiveness of the the adult age verification requirement in the context of the global internet was addressed in the U.S. Supreme Court decision on COPA. The Court stated:[7]

  > (A) filter can prevent minors from seeing all pornography, not just pornography posted to the Web from America. . . . COPA does not prevent minors from having access to those foreign harmful materials. . . . [I]f COPA is upheld, . . . providers of the materials that would be covered by the statute simply can move their operations overseas.

  - If U.S. sites are required to implement age and identity verification, young people will simply use a "door" to the site from another country or migrate to a site that is located in another country.

- Other countries could follow the lead of the U.S. in requiring digital identification for users of social networking sties. The New York Times recently published an article that outlined how young people in Egypt are using Facebook for political organizing.[8] In the U.S. in the 1990, filtering was promoted as the solution to protect young people from accessing online pornography. Other countries are using filtering to prevent their residents from accessing any sites that promote human rights and democracy.

  - There are very important reasons to protect privacy online.

- Many of the authentication approaches would require wide acceptance, which would be very costly. Given the current data on online risks, as well as the likelihood of limited benefits derived from these approaches, the costs would not be justified.

  - It is necessary to document that there is a reasonable likelihood of success in achieving the desired outcomes before moving forward to implement a protection approach. The Attorneys General have not provided any data that documents the specific risks of sexual predation on social networking sites. No analysis has been done of costs.

- The research data clearly demonstrates that teens face greater risk from their peers - including sexual harassment, sexual solicitation, cyberbullying, use of technologies by abusive partners. Separating minors from adults will do nothing to address these significant risks and would likely lead to false security that something has been done to address online concerns, when the concerns are still present.

  - It is necessary to effectively educate young people and their parents about the risks and effective prevention and intervention approaches.

---

5 http://cyber.law.harvard.edu/research/isttf/TAB. Note submission of Microsoft and eGuardian.
6 Digital Playgrounds: Creating Safer Online Environments for Youth. download.microsoft.com/download/2/8/4/284093f4-5058-4a32-bf13-c12e2320cd73/Digital%20Playground.pdf
7 ACLU v. Gonzales, (2007) 535 U.S. 564, 667.
8 Shapiro, S.M. Revolution, Facebook Style, (January 22, 2009) The New York Times. http://www.nytimes.com/2009/01/25/magazine/25bloggers-t.html

- Most teens turn 18 during their senior year of high school. There is no evidence whatsoever that at this point in time they mysteriously turn into potentially dangerous sexual predators who must be prevented from communicating with their slightly younger peers.

  - Older teens are far more savvy and can provide very valuable guidance to their younger peers and siblings. Seeking to empower these older teens to be effective mentors and take responsibility for the well-being of others online will be a very effective risk prevention approach.

- Trying to build a better “Internet mouse trap,” simply leads to “smarter mice.” For evidence of this, conduct a search on the term “bypass Internet filter.” The returns provide an excellent example of the lack of effectiveness of the last great technology “quick fix” - filtering software. Teens will not “buy in” to an approach that requires they stop communicating with people they know to be perfectly safe.

  - It is not possible to keep teens in electronically fenced play-yards. Given their significantly greater technical expertise they will easily defeat any age and identity verification system developed.

- Adult age verification, especially when used for financial transactions can be effective because adults are motivated to protect their identification. Given that the case has not been made that massive numbers of young people are at risk from sexual predators and that to address this concern it is necessary for everyone to present accurate identification, there would be ample motivation to defeat any system - which would be easy to accomplish.

  - Voluntary compliance is highly unlikely. Mandatory compliance would lead to massive protest and immediate development of strategies to defeat the requirement.

- In the area of sexual predation, young people have always faced greater risk from family members and acquaintances. The focus on “online stranger danger” has led to a failure to recognize that many of these sexual abusers may now be using interactive technologies to groom and control older victims and to create and disseminate child pornography. Parents would likely allow exceptions to the online communications limitations - and allow their child to communicate with people like uncles, coaches, church group leaders, and the like who, based on the data, are far more likely to present risks.

  - It is essential that we address all forms of sexual risk to young people and move beyond the undue attention to potentially dangerous online strangers.

- Implementation of an age and identify verification program would clearly place young people at greater risk. Currently, many teens are careful to limit their friendship links to people they know in the real world. If age and identify verification systems are put into place, young people and their parents would be more likely to think it is safe to communicate with people they do not know in the real world, thinking that these they have been accurately “identified.” Nefarious individuals could easily obtain a false digital identification. While the current data indicates that sexual predators rarely are deceptive about their age, use of age and identify verification would likely increase the level of deception.

  - The false security that comes from reliance on technology “quick fixes” can lead to significant harmful unintended consequences.

- The research demonstrates that the young people who are at the greatest risk online are the ones who are already at greater risk in the real world. This means they are far more likely to intentionally engage in risky behavior, have peers who support risky behavior, and have parents who are ineffectively involved. These young people will be the first to bypass any age and identity verification systems. Further, most of the age and identity verification technologies presented required voluntary compliance and active involvement of parents, which is far less likely to occur for most at risk youth.

  - To effectively address the concerns of the most at risk youth will require implementing approaches that are grounded in effective adolescent risk prevention.

- Young people face far greater risks of sexual abuse from people they know - family members and acquaintances. Any identification system would necessarily allow for some adult contact - for example a

parent who wants to establish a friendship link for monitoring purposes. This exemption process would allow potentially very dangerous adults convenient access to victims, under an aura of safety.

  - The concerns of false security are real.

- Two digital identification companies are already taking advantage of the pressure by the Attorneys General to implement age and identity identification, eGuardian and Identity.net.[9] These companies are asking schools to verify the identity of students. They promise this will protect students from online predators. What they are not telling educators or parents is that their business model involves creating a unique persistent identifier that is associated with demographic data that can be provided to partner sites to enable those sites to engage in more in-depth profiling to be used to target advertising to young people.

  - In our zeal to protect a few young people from online sexual predators, we should not turn all other young people, as well as adults, over to the market profiling and advertising "predators."

- Another digital identification company, Aristotle/Integrity, which served on the Task Force, has a business model that presents even greater concerns.[10] Aristotle maintains databases on voters which it has combined with other data to allow micro-targeting of voters based on demographics, interests, as well as voter records. The companion company, Integrity, uses this database for age verification.

  - If this company were in a position to digitally identify users of social networking sites, the amount of personal interest, activities, and connections data that it could aggregate and sell to candidates of its choosing would be massive - and frightening.

- There are effective desk-top protection technologies that parents can easily use to restrict their children's access to specific sites, such as the Microsoft Vista Family Controls. These technologies accomplish everything that the Attorneys General desire to occur from the perspective of preventing children under the age of 13 from joining teen sites. The protective features on the social networking sites appear to be working effectively. If a teen uses the protective features, no one can contact that teen unless that person has additional information, such as the teen's real name. Further, no one can see the teen's profile without being approved by the teen as a "friend." Teens appear to be using these protective features.[11]

  - The continued development of desk top protections, protection features on children and teen sites, and education provided to parents, children, and teens on the use of these protective features is clearly the most productive path to follow.

As a former U.S. Attorney General. Dick Thornbough stated in the preface of another report addressing youth risk online, *Youth Pornography and the Internet*:

> [This report] will disappoint those who expect a technological "quick fix" to the challenge of pornography on the Internet. ... It will disappoint parents, school officials, and librarians who seek surrogates to fulfill the responsibilities of training and supervision needed to truly protect children from inappropriate sexual materials on the Internet.[12]

The Berkman Task Force Report has apparently disappointed some Attorneys General, hopefully a minority, who were expecting a technological "quick fix" to the challenge of online sexual solicitation and other online risks. This Report will clearly disappoint anyone thinking that age and identity verification can serve as surrogate for the implementation of a comprehensive approach that involves effective technology protections, education, parent involvement, and comprehensive risk prevention.

---

[9] Davis, M. R (November 11, 2008) Firms Verify Online IDs Via Schools. Education Week. http://www.edweek.org/ew/articles/2008/11/12/12social_ep.h28.html.

[10] http://www.aristotle.com.

[11] A Pew Internet and American Life report issued in April 2007 revealed that 66% of teens with profiles on social networking sites say they limit access to their profile in some way so that it is not visible to all internet users. Lenhart, A., et. al. (December 19, 2007) Teens and Social Media. Pew Internet and American Life. http://www.pewinternet.org/PPF/r/230/report_display.asp.

[12] Thornburgh, D & Lin, H., (2002) *Youth, Pornography and the Internet*. National Academy Press. http:// books.nap.edu/openbook.php?isbn=0309082749&page=R1.