Introducing Digi-Parent

And Comments on the Effectiveness of Technology Approaches to Address Human Behavior Concerns

Nancy Willard, M.S., J.D.
Center for Safe and Responsible Internet Use
Presentation to the Berkman Internet Safety Technical Task Force
September 23, 2008

Introducing Digi-Parent

Digi-Parent sits by a child's computer screen so it can conveniently look over the shoulder of its child. The Digi-Parent can read terms of use agreements and privacy policies and discuss these in relation to important values. It can make sure its child has implemented all of the protection features on social networking sites and instant messaging. It will review the profiles of all of its child's friends to make sure they are safe, as well as the material posted by its child and its child's friends. It has been programmed to recognize all of the possible words and phrases that could be used to sexually solicit or cyberbully a child. It even knows how much homework a child so it can turn off the computer to ensure its completion. The advanced model can be used with "at risk" youth. This model will be programmed to say things like "I love you" "How was your day? "How are you feeling?" "You look a bit sad, is anything wrong?" "You know you can come to me if you have any problems."

Digi-Parent - the technology "quick fix" for the lack of an effectively engaged parent!!!

> "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]
>
> "[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.[2]

Technology "Quick Fixes"

An ineffective technology solution that seeks to control the intentional behavior of teens online because of concerns related to safety or responsible use.

Technology Protections

An effective technology protection solution designed to protect against harm coming from the outside or accidental behavior.

Techno-Panic

A heightened level of concern about the use of contemporary technologies by young people that is disproportionate to the empirical data on the degree of risk.

The Porn Techno-Panic

- Reliance on filtering has lead to …
  - Increased accidental access due to failure to educate.
  - Filtering companies making blocking decisions based on inappropriate bias.
  - Teens can easily bypass the filter.
  - Schools failed to implement effective management.
  - Teachers/students unable to access appropriate sites.
  - Safe school personnel unable to review online material that raises concerns on student safety.

Accountability

- What is the data about risk and what are the implications?
- How feasible are the proposed technical solutions?
- Is there a substantial likelihood a solution will effectively address the concerns and not lead to unintended consequences?

What is the data about risk and what are the implications?

- The young people who are at the greatest risk online are the ones who are already at greatest risk in the real world.[3]
  - Will engage in risk-taking behavior.
  - Do not have effectively engaged parents.
- The greatest risks to young people come from people they know ~ especially other young people.[4]
  - Attempting to wall them off from strange adults will not effectively address the concerns.
  - The concern is NOT "stranger danger."
- The vast majority of teens report effective responses to negative online incidents and lack of distress.[5]
  - Young people do not perceive the Internet is exceptionally dangerous.
  - Many appear to have a healthy understanding of the real risks.
- Teens are not reporting negative online incidents to adults.[6]
  - In many cases this is because they handled the incident effectively.
  - But teens are also do not report online concerns because of fear getting into trouble and losing Internet use.
  - The Techno-Panic is likely increasing the reluctance to report concerns to adults.
- Teens whose parents are actively and positively involved engage in far less risky online behavior.[7]
  - No technology "quick fix" can substitute for an actively and positively involved parent.
  - Actively and positively involved parents do not need "quick fixes."
  - The Techno-Panic can reduce the degree to which parents are positively involved.
- It appears that a significant number of pre-teens (<10) are using social networking sites.[8]
  - It appears that the majority of their parents know and have approved.
  - It appears that as the social networking sites have increased their protective features, more parents are approving use by pre-teens.
- There has been an unconscionable overhyping of data or presentation of inaccurate data by some media, politicians, companies, and advocacy groups.[9]
  - 1 in 5 children sexually solicited.
  - 50,000 predators at any time on social networking sites.
- The Attorneys General have no incident data to support the argument that social networking sites are especially dangerous.[10]
  - Predator "stings" appear to occur in chat rooms.
  - How can they say that social networking sites are exceptionally dangerous if they have no data to support this?

How feasible are the proposed technical solutions?

- To digitally identify someone requires a "trusted authority" to verify identity and age.
  - *No such trusted authority exists and it would be very expensive to set this up.*
- An approach that requires parents to obtain a digital identification of their child requires a Trusted Authority that can accurately validate custodial authority.
  - *No such trusted authority exists and it would be very expensive to set this up and impossible to keep it updated.*
- Digital identification would have to be global or young people would simply enter the sites from another country.
  - *The U.S. does not control the world.*
- The approach would have to be universal, requiring digital identification of all users or minors will simply sign up as adults and lose the benefits of the protective features.
  - *Social networking site users would not be happy, especially when there is no data on the degree of concern.*
- An approach that encourages teens to voluntarily limit their access to sites limited to minors would require that teens believe the social networking sites are extraordinarily dangerous and they are incapable of protecting themselves.
  - *Good luck*!
- An approach that seeks to prevent pre-teens from establishing accounts by requiring verified parent approval would require that parents believe that the social networking sites are extraordinarily dangerous and they are incapable of protecting their child.
  - *Good luck!*
- An approach that sets up COPPA-compliant social networking sites for pre-teens that are subscription-based, requiring parents to pay a modest price using a credit card and preventing market profiling and advertising appears feasible.
  - *But the pre-teens are going to want to be on the popular sites.*

Is there a substantial likelihood a proposed solution will effectively address the concerns and not lead to unintended consequences?

- Establishing a digital identification for minors would be …
  - Impossible without the creation of a RealID program for minors.
  - Far too costly.
  - Unreliable because of the difficulty of establishing current custodial authority.
  - Exceptionally easy to scam.

- Requiring all minors to obtain verified parental approval would result in …
  - Minors registering as adults and losing all protections.
  - Minors registering through another country.
  - Minors faking parent approval.
  - Parents approving pre-teens.
  - Increasing the perception of teens that adults have "gone off the deep-end" and can't be trusted.
- Requiring all U.S. social networking site users to digitally identify themselves would result in users.
  - Registering through another country.
  - Aggressive efforts to undermine the entire digital identification industry.
- SUGGESTING that all social networking site users should digitally identify themselves would result in …
  - Aggressive efforts to undermine the entire digital identification industry.
  - Vicious rumors of ulterior motives.
  - Profiling, Homeland Security, Revelations 13.
  - Because AGs have no data to support their argument that sites are dangerous for all minors.
- Trying to protect minors by walling them off from adults will not protect them and could harm them.
  - The greatest risks to minors ~ sexual, cyberbullying, unsafe or dangerous communities ~ are from their peers or adults they know.
  - Thinking that minors are protected because they have been walled off from contact with adult strangers will lead to false security and failure to address the greater risks!
- Trying to control the online behavior of teens with "parental empowerment tools" will never be effective.
  - Because it is developmentally inappropriate and technically impossible to keep teens in "electronically fenced play-yards."
- Setting up systems for parents to register their children's email addresses to prevent them from registering on sites will not be effective because ...
  - A teen or pre-teen can create a new email account in less than a minute.
  - Most parents know and have approved the use of these sites by their teens and pre-teens.
- Strong efforts to keep pre-teens off of social networking sites are unlikely to be successful because …
  - Parents think these sites are safe ~ and with proper precautions they ARE SAFE.
  - Would require significant FEAR-MONGERING that is unsupported by the data.
- Promoting the need for technology "quick fixes" will require significant unsubstantiated fear-mongering, which will place teens at greater risk.
  - Because the fear-mongering will lead teens to avoid talking with adults about real online concerns.
- Promoting the need for technology "quick fixes" will require significant unsubstantiated fear-mongering which will undermine the credibility of the fear-mongers.
  - Because ALL of the data argues against the effectiveness of a technology "quick fix" approach.
- It appears that the "user empowerment tools" in the form of protective features on these sites ARE working effectively.
  - Making them default will increase usage.
  - Must pay attention to research and listen to teens to improve protective features.
  - Creatively use "social norms" approaches to encourage use.
- Establishing social networking sites for pre-teens appears to be a good idea.
  - But pre-teens really want to be on the "cool, popular" sites …
  - Which their parents think are safe …
  - Which, with proper precautions, ARE SAFE.
- The best ways to protect young people online remain education and effectively engaged parenting.
  - But the excessive, unjustified FEAR-MONGERING has resulted in many young people who are no longer trusting adults.
  - And this approach will not effectively address the concerns presented by the more "at risk" youth.

Recommendations

- Increase use and ensure effectiveness of the user empowerment protection features on all general purpose sites attracting youth.
  - Need more research.
  - Focus on social norms approaches to increase use.
- Encourage the development of COPPA-compliant social networking sites for pre-teens.
  - Subscription, no profiling.
  - Greater protections, such as notice to parent's email if new friend or public post.
- Encourage popular sites to create pre-teen section.
  - Provide option for parents to approve interactions with older users.
- Stop the fear-mongering.
- Provide effective education.
- Encourage peer leadership, since many teens are no longer listening to adults.
- Implement a comprehensive approach to address youth risk online within the context of current effective approaches to address youth risk.

About the Author

Nancy Willard, M.S., J.D. is the director of the Center for Safe and Responsible Internet Use - http://csriu.org. 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 Safety 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.

Endnotes

[1] Naisbitt, J., Megatrends: Ten new directions transforming our lives, New York, N.Y. Warner Books, 1984.
[2] Thornburgh, D & Lin, H., (2002) Youth, Pornography and the Internet. National Academy Press. http://books.nap.edu/openbook.php?isbn=0309082749&page=R1.
[3] 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; 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.
[4] Wolak, J., Mitchell, K., and Finkelhor, D. (2006). Online victimization of youth: Five years later. National Center for Missing & Exploited Children Bulletin - #07-06-025. Alexandria, VA. http://www.unh.edu/ccrc/internet-crimes/papers.html; 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; McQuade, S. (2008) A Survey of Internet and At-risk Behaviors. Rochester Institute of Technology. http://www.rrcsei.org.
[5] Wolak, J., Mitchell, K., and Finkelhor, D. (2006); Rosen, L. D., et al., (2008).
[6] Wolak, J., Mitchell, K., and Finkelhor, D. (2006).
[7] Rosen, L. D., et al., (2008).
[8] There is no study on this. Data in Rosen (2008 suggests this. Further insight provided through electronic communications with school librarians through LM-Net discussion list.
[9] Oft-quoted data that 1 in 7 young people are sexually solicited online leaves out critically important findings. The report asked about unwanted sexual related communications. Most of these communications came from other teens. 4 of 5 teens are sexually harassed in high school. Only 33% of these solicitations were distressing to the recipient. 16% of the solicitations were from females; 49% of whom were under 18. Only 9% of the solicitations were from people over the age of 25; 92% male, the others gender unknown. "It has been estimated that, at any given time, 50,000 predators are on the Internet prowling for children," U.S. Attorney General Gonzales in a press conference. “It is estimated that, at any given moment, 50,000 predators are prowling for children online, many of whom are lurking within social networks. Representative Upton in the House Congressional Record: July 26, 2006 in support of the Deleting Online Predators Act. Gonzales apparently got his data from Dateline’s To Catch a Predator. Dateline said they got this figure from a FBI authority ~ who has denied providing this figure. Dateline created this figure out of “thin air.”
[10] I asked for the data.