



Social Networking and Age Verification: Many Hard Questions; No Easy Solutions

by Adam Thierer*

Introduction

Two years ago, few people were talking about “social networking” websites. Today, however, social networking sites are among the most-trafficked on the Internet. Concerns about how youngsters use these services have already prompted lawmakers to introduce legislation to ban access to such sites in schools and libraries. Others, including several state attorneys general, want such sites to age-verify all users to exclude those over or under a certain age.

“Social networking” defies easy definition because, in many ways, the Internet and most of the websites that make up the World Wide Web have been fundamentally tied up with the notion of social networking from their inception. “Trying to define social networking is very much like trying to pin down a moving target, because it’s evolving so quickly,” argue Larry Magid and Anne Collier, authors of *MySpace Unraveled: A Parent’s Guide to Teen Social Networking*.¹

Nonetheless, more formal social networking sites began popping up a few years ago that offered their users the space and tools to build the equivalent of an online journal and then to network with others more easily. MySpace, Facebook, Xanga, Bebo, Hi5, Friendster, Tagged, Imbee, LiveJournal, Yahoo 360, and Windows Live Spaces are just a few of the hundreds of social networking sites online today.² New sites are seemingly surfacing every week, and they are growing more personalized in an attempt to appeal to specific niches.³ For example, in late 2006, a new site for younger government workers (www.youngfeds.org) was launched that bills itself as “the home for the views and voices that matter to young people working in and around the federal

* Adam Thierer (athierer@pff.org) is a senior fellow with The Progress & Freedom Foundation and the director of its Center for Digital Media Freedom. The views expressed in this report are his own. The author wishes to thank John J. Cardillo of Sentinel, Jeff Schmidt of Authis, Denise G. Tayloe of Privo, Anne Collier of Net Family News, and Tim Lordan of the Internet Education Foundation for their valuable input on various matters discussed in this paper.

¹ Larry Magid and Anne Collier, *MySpace Unraveled: A Parent’s Guide to Teen Social Networking* (Berkeley, CA: Peachtree Press, 2007), p. 2.

² For a list of notable social networking sites, see:
http://en.wikipedia.org/wiki/List_of_social_networking_websites

³ See Robert D. Hof, “There’s Not Enough ‘Me’ in MySpace,” *Business Week*, December 4, 2006, p. 40.

government.”⁴

At the heart of the debate over social networking lie the same concerns that have motivated previous Internet regulatory initiatives: underage access to objectionable material and fears about child predators. Calls for regulation have followed. In the past session of Congress, former Rep. Michael Fitzpatrick (R-PA) introduced the Deleting Online Predators Act (DOPA), which proposed a ban on social networking sites in public schools and libraries. Fitzpatrick argued that such sites are a “virtual hunting ground for sexual predators.”⁵ Others in Congress were eager to act as well. In fact, in the span of just one month in summer 2006, the House Energy and Commerce Committee alone held four hearings on the issue of sexual exploitation of children on the Internet.⁶ At those hearings, several witnesses and lawmakers called for increased government oversight or regulation of the Internet and social networking websites in particular.⁷

Unsurprisingly, DOPA passed the House of Representatives shortly thereafter by a lopsided 410-15 vote.⁸ And DOPA was reintroduced just a few weeks into the current session of Congress by Senator Ted Stevens (R-AK), the ranking minority member and former chairman of the Senate Commerce Committee.⁹ It is section 2 of a new bill that Sen. Stevens has sponsored and that is titled the “Protecting Children in the 21st Century Act” (S. 49).¹⁰

Many state attorneys general (AGs) are also expressing concern and some have suggested that legal action against social networking sites might be forthcoming. Connecticut Attorney General Richard Blumenthal has been a particularly vociferous critic, calling social networking sites “a sexual predator’s dream and a parent’s worst nightmare.”¹¹ Many AGs such as Blumenthal and North Carolina Attorney General Roy Cooper are pressuring social networking sites to authenticate the identities of their users. Specifically, AGs want site operators to verify the age of all their users to keep anyone under the age of 16 or 18 off those sites entirely. Some also propose raising the

⁴ Stephen Barr, “Fostering a Facebook for the Feds,” *Washington Post*, October 23, 2006, p. D1.

⁵ Letter from Rep. Michael Fitzpatrick (R-PA) to Rep. Frank Wolf (R-VA), chairman of the House Committee on Financial Services Subcommittee on Science, State, Justice and Commerce, June 7, 2006, <http://fitzpatrick.house.gov/UploadedFiles/Letter%20Wolf.pdf>

⁶ “Sexual Exploitation of Children over the Internet,” *Staff Report*, Committee on Energy and Commerce, U.S. House of Representatives, 109th Congress, January 2007, http://republicans.energycommerce.house.gov/108/News/01032007_Report.pdf

⁷ Larry Magid notes that “DOPA does nothing to strengthen penalties or increase prosecution of criminals who prey on children. Instead, it punishes the potential victims and educational institutions chartered to serve them, by denying access to interactive sites at school and libraries. It would be like trying to protect children from being injured or killed by drunk drivers by ruling that kids can no longer walk, ride a bike or even ride in a car or bus to school.” Larry Magid, “House Misfires on Internet Safety,” *CBS News.com*, August 1, 2006,

www.cbsnews.com/stories/2006/08/01/scitech/pcanswer/main1853357.shtml

⁸ Declan McCullagh, “Chat Rooms Could Face Expulsion,” *CNet News.com*, July 28, 2006, http://news.com.com/2100-1028_3-6099414.html?part=rss&tag=6099414&subj=news

⁹ Anne Broache, “Congress Off to Slow Start with Tech,” *ZDNet News*, January 9, 2007, http://news.zdnet.com/2100-9588_22-6148312.html

¹⁰ http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:s49is.txt.pdf

¹¹ Quoted in McCullagh, *op. cit.*

minimum allowable age to access the sites. But those AGs haven't offered a specific age verification solution themselves; they are simply demanding that social networking providers find a way to do it effectively.¹²

The fact that AGs have demanded that others devise a workable age verification solution without proposing any solutions themselves is not surprising. Age verification is extremely complicated, and it would be even more complicated in this case because public officials are demanding the age verification of minors as well as adults, which presents a wide array of special challenges and concerns.¹³

This paper will discuss some of those challenges and concerns and will raise a host of questions that need to be carefully considered as both lawmakers and the industry move forward. The study offers three general conclusions:

- (1) Age verification raises **many sensitive issues related to the privacy of children and online freedom of speech and expression**. We need to avoid a rushed solution that too easily compromises those values.
- (2) In all likelihood, even if a technical solution emerges that satisfies that first goal, it will almost certainly not be foolproof. **Perfect age verification is a quixotic objective**. It is important that we do not rush into a solution that provides a false sense of security to either parents or the youngsters using social networking sites. And it is important that we do nothing that could force mainstream, domestic social networking sites offshore or, even worse, that could drive the users we are trying to protect to offshore sites. Whatever their concerns are about current domestic sites, parents and policy makers should understand that those sites are generally more accountable and visible than offshore sites over which we have virtually no influence but that have the same reach as domestic sites.
- (3) In light of (1) and (2), **education is absolutely essential**. Parents, schools, government, other institutions, and web site operators all need to do much more to educate youngsters about online safety and proper etiquette within interactive environments.

In the end, a mix of solutions—some technical, but more education based—will likely provide the optimal solution to concerns about online child safety. The technological solutions should be developed by the private sector. The education solutions need to be developed and distributed through a partnership of private-sector, nonprofit, and government entities.

The role of law enforcement should be to focus on prosecuting serious threats

¹² See Emily Steel and Julia Angwin, "MySpace Receives More Pressure to Limit Children's Access to Site," *Wall Street Journal*, June 23, 2006, http://online.wsj.com/public/article/SB115102268445288250-YRxt0rTsyf1QiQf2EPBYSf7iU_20070624.html?mod=tff_main_tff_top

¹³ For a general overview of age verification challenges, see Anick Jesdanun, "Age Verification at Social-Network Sites Could Prove Difficult," *Associated Press Financial Wire*, July 14, 2006.

that are discovered online. Appropriate sentencing is the most important part of that solution. Shockingly, a 2003 Department of Justice study reported that the average sentence for child molesters was approximately seven years; on average, they were released after serving just three of those seven years.¹⁴ Such sentences need to be greatly extended and enforced to ensure that convicted child abusers aren't out on the streets and sitting behind keyboards looking to prey upon children again.¹⁵ But it is also essential that law enforcement officials receive the resources and training necessary to adequately monitor online networks for predators and to bring them to justice when they are found.¹⁶

Finally, it goes without saying that there is no substitute for good parenting and mentoring of our kids. We should not be calling in government to act as surrogate parent when parents already have the tools and the ability to handle much of this problem themselves.

Putting the Problem in Perspective

Before detailing the concerns associated with age verification, we need to begin with some basic assumptions about the problems we want to solve and the challenges we will likely face in attempting to do so. At root, the two problems that most critics or lawmakers point to with regard to social networking sites are:

- (1) The “bad people” problem: namely, child predators. That might also include cyber-stalkers or cyber-bullies.
- (2) The “bad pictures” problem: specifically, pornography, but that can include other images and content considered unsuitable for minors.

Those two issues are getting conflated in the debate about social networking. That is unfortunate because they are two very different problems, and each poses special challenges in its own right. Moreover, most people would likely agree that the first problem—protecting children from predators—deserves more attention and resources than the latter. Moreover, the latter problem does not necessarily require age

¹⁴ “5 Percent of Sex Offenders Rearrested for Another Sex Crime within 3 Years of Prison Release,” U.S. Department of Justice, Office of Justice Programs, November 16, 2003, www.ojp.usdoj.gov/bjs/pub/press/rsorp94pr.htm

¹⁵ President Bush recently signed the “Adam Walsh Child Protection and Safety Act of 2006,” which increases mandatory minimum sentences for various crimes against children. See “President Signs H.R. 4472, the Adam Walsh Child Protection and Safety Act of 2006,” White House *Press Release*, July 27, 2006, www.whitehouse.gov/news/releases/2006/07/20060727-6.html

¹⁶ Senators John McCain (R-AZ) and Charles Schumer (D-NY) recently introduced legislation, S. 519, that would require all convicted sex offenders to register their e-mail addresses with law enforcement officials so that their online activities could be monitored. The e-mail addresses could also be monitored by social networking sites to ensure sex offenders were not on those sites. While there is nothing stopping offenders from changing their e-mails to avoid detection, the legislation also stipulates that any offender caught doing so will be eligible for an additional 10 years of jail time on top of the sentence for any other underlying offense.

verification solutions; it can be addressed in other ways.

A National Child Abduction Epidemic? This essay will focus primarily on the “bad people” problem because it is prompting the most calls for regulation of social networking sites. It is important, however, to be realistic about the scope of this problem. This debate is being driven by fear—fear of bad guys lurking online and waiting to snatch up our children. Indeed, there have been a handful of highly publicized cases of minors being contacted and later abducted or abused by child predators on social networking sites.¹⁷ Such cases do not mean that a national epidemic of Internet-related child abductions is occurring.

Generally speaking, abductions by strangers “represent an extremely small portion of all missing children [cases].” That conclusion was one of the central findings of the 2002 *National Incidence Studies of Missing, Abducted, Runaway, and Thrownaway Children* (NISMART), a study conducted by the Department of Justice’s Office of Juvenile Justice and Delinquency Prevention.¹⁸ Although the survey is several years old and suffers from some data and methodological deficiencies, it remains the most comprehensive survey of missing and abducted children in the United States.

The NISMART survey broke down juvenile abductions into two categories—family versus non-family. It found that the vast majority of kidnapping victims were abducted by family, friends of the family, or people who had a close relationships with (or the trust of) the minors. Only 115 of the estimated 260,000 abductions—or less than a tenth of a percent—fit the stereotypical abduction scenario that parents most fear: complete strangers snatching children and transporting them miles away.¹⁹ Despite that finding, public policy debates and media reports remain preoccupied with the horror stories about abductions by random strangers, leaving the impression that the problem is much larger than the more serious issues of family or acquaintance abductions.²⁰

¹⁷ Claire Osborn, “Teen, Mom Sue MySpace.com for \$30 Million,” *Austin American-Statesman*, June 20, 2006.

¹⁸ Andrea J. Sedlak, David Finkelhor, Heather Hammer, and Dana J. Schultz, “National Estimate of Missing Children: An Overview,” *National Incidence Studies of Missing, Abducted, Runaway, and Thrownaway Children* (NISMART), October 2002, p. 7, www.missingkids.com/en_US/documents/nismart2_overview.pdf

¹⁹ A recent study of cases about missing children in Ohio revealed a similar trend. Of the 11,074 documented missing child cases in 2005, just 5 involved abduction by strangers compared to 146 abductions by family members. *2005 Annual Report*, Ohio Missing Children Clearinghouse, p. 4; www.ag.state.oh.us/victim/pubs/2005ann_rept_mcc.pdf

²⁰ Indeed, one recent study suggests that perception has replaced reality in the minds of many in the press and general public, who have increasingly come to believe that stranger abductions account for most missing child incidents. A 2006 analysis of *New York Times* articles about kidnappings, by Glenn W. Muschert, Melissa Young-Spillers, and Dawn Carr in the *Justice Policy Journal*, argued that “the *Times* disproportionately focuses on stereotypical kidnapping incidents, while social science data suggest that familial abductions are far more prevalent.” And abduction estimates made by some activists were also “highly exaggerated,” they found. Unsurprisingly, for those reasons, the authors note that various public opinion polls have revealed that most people believed that abductions by strangers accounted for most missing child cases even though the exact opposite was true. Glenn W. Muschert, Melissa Young-Spillers, and Dawn Carr, *Justice Policy Journal*, vol. 3, no. 2, Fall 2006, pp. 4-6.

Research has shown that this conclusion is also true of child abuse and sex offenders in general, not just abductions. As psychologist Anna C. Salter, author of *Predators: Pedophiles, Rapists, and Other Sex Offenders*, points out, “[Sex offenders] are part of our communities, part of our network of friends, worse yet, sometimes part of our families.”²¹ And former FBI Special Agent Kenneth V. Lanning, author of *Child Molesters: A Behavior Analysis*, notes the following:

The often forgotten piece in the puzzle of the sexual victimization of children is acquaintance molestation. This seems to be the most difficult manifestation of the problem for society and the law to face. People seem more willing to accept a sinister stranger from a different location or father/stepfather from a different socioeconomic background as a child molester than a clergy member, next-door neighbor, law-enforcement officer, pediatrician, teacher, or volunteer with direct access to children. The acquaintance molester, by definition, is one of us. He is not just an external threat. We cannot easily distinguish him from us or identify him by physical traits. These kinds of molesters have always existed, but society and the criminal-justice system have been reluctant to accept the reality of these cases.²²

Clearly, the problem of family and acquaintance abductions and sex abuse predated the rise of the Internet, and it will unlikely be diminished by age verification of minors on social networking websites. But the argument could be made that abductions by strangers—while exceedingly rare—could be reduced even further by age-verifying minors or adults before they enter certain sites.

This potential reduction may be true, but it is important to remember that predators can’t magically reach through a computer screen and grab our kids. Predators must meet them somewhere in the physical world (i.e., a mall, park, playground, etc.) The danger of the Internet is that it allows predators to groom minors over a protracted period, while doing so *from a distance*. But the fact that they are doing so from a distance—and over electronic communications networks, no less—means that we have actually gained some important advantages in our effort to combat child predation. Many of the predators leave digital tracks for us to follow. Thus, to the extent that disturbing things are happening online or being facilitated by the Internet in any fashion, at least there is a digital record of those activities or crimes. The electronic tracks have made it easier to recover children or to track perpetrators on many occasions.²³

²¹ “Sex offenders only very rarely sneak into a house in the middle of the night. More often they come through the front door in the day, as friends and neighbors, as Boy Scout leaders, priests, principals, teachers, doctors, and coaches. They are invited into our homes time after time, and we give them permission to take our children on the overnight camping trip, the basketball game, or down to the Salvation Army post for youth activities.” Anna C. Salter, *Predators: Pedophiles, Rapists, and Other Sex Offenders* (New York: Basic Books, 2003), p. 5, 76.

²² Kenneth V. Lanning, *Child Molesters: A Behavior Analysis*, National Center for Missing & Exploited Children, 2001, www.missingkids.com/missingkids/servlet/ResourceServlet?LanguageCountry=en_US&PageId=469

²³ See Mark Sherman, “Chat Rooms Help FBI Hunt for Pedophiles,” *USA Today*, May 15, 2006, www.usatoday.com/tech/news/2006-05-15-fbi-chat-rooms_x.htm

Of course, digital records have also made it easier to catch minors engaging in foolish behavior after they post information or photos about their actions online.²⁴ In past generations, parents often warned their kids to behave themselves in public or else “it will go down on your permanent record.” It was largely just a scare tactic, because there really was no permanent record of the mundane activities of youth. Today, however—for better or for worse—*the Internet is becoming “your permanent record.”* No doubt, this raises some serious, long-term privacy concerns. But the one positive aspect is that the existence of electronic records makes it easier for parents, website operators or law enforcement officials to deal with online troublemakers of all varieties.²⁵ (As will be discussed at greater length below, this is why education is essential to make sure both kids and their parents understand that serious consequences are associated with what they post online).

“At-Risk” Youth are the Real Concern: Not only is it a myth that there is a growing epidemic of Internet-facilitated child abductions, but it is also a myth that all children are equally susceptible to falling prey to online predators. In reality, the population of “at-risk” youngsters who are most likely to become the victim of online predators is very small.

A 2004 study by researchers from the University of New Hampshire’s Crimes against Children Research Center surveyed more than 2,500 cases in which juveniles became the victims of sex crimes by people they met through the Internet.²⁶ The authors found that those children—almost all of whom were teenagers—were not, generally speaking, the victims of the stereotypical scenario that most parents and policy makers fear: “strangers who are pedophiles and who deceive and lure children, frequently over long distances, into situations where they can be forcibly abducted or sexually assaulted.”²⁷ In fact, the opposite was the case.

The study found that “although they undoubtedly manipulated juveniles in a variety of ways, the offenders in the Internet-initiated crimes did not generally deceive victims about being older adults who were interested in sexual relationships. Victims usually knew this propensity before their first face-to-face encounters with offenders.”²⁸ The survey results supporting this finding are startling:

²⁴ Wendy Davis, “Teens’ Online Postings Are New Tool for Police,” *Boston Globe*, May 15, 2006, www.boston.com/news/nation/articles/2006/05/15/teens_online_postings_are_new_tool_for_police;

Andrew L. Wang, “Teen Blog Watch is On,” *Chicago Tribune*, May 23, 2006.

²⁵ Eric Tucker, “Police Departments Turning to YouTube to Catch Suspects,” *Boston Globe*, February 24, 2007, www.boston.com/news/local/rhode_island/articles/2007/02/24/police_departments_turning_to_youtube_to_catch_suspects

²⁶ Janis Wolak, David Finkelhor, and Kimberly Mitchell, “Internet-initiated Sex Crimes against Minors: Implications for Prevention Based on Findings from a National Study,” *Journal of Adolescent Health*, vol. 35, no. 5, 2004, pp. 11-20, www.unh.edu/ccrc/pdf/CV71.pdf

²⁷ *Ibid.*, p. 18.

²⁸ *Ibid.*

- Only 5% of the adult offenders lied about their age and tried to pass themselves as being minors.
- Only 21% of the adult offenders lied about their sexual desires with the minor.

Yet, despite the fact that most offenders did not hide their desires:

- The great majority of victims (83%) who met with offenders face-to-face voluntarily went somewhere with them afterward (a hotel, movie, restaurant, etc.), and many (41%) spent at least one night with the offender.
- Most victims (73%) willingly met with offenders more than once.
- In 89% of the cases, the victims willingly engaged in some sort of sexual activity with the offender; only 5% of the cases involved violence or rape.

That those children would consent to meet with older strangers and engage in such acts is shocking and disturbing, and most parents would find it unfathomable that their own children would voluntarily involve themselves with older men in this fashion. But therein lies the real problem. The researchers in this study found most youngsters involved in those cases did not have a good relationship with their parents. In many cases, the victims reported a high degree of conflict with their parents or very little parental interaction and mentoring. In some cases, parents were absent from the home altogether. Loneliness and depression were also prevalent traits in many of the youngsters. And some of the boys who became willing victims were “gay or questioning” about their sexuality and were scared to talk to the parents or educators about it.

Those children are at-risk youth who need help. What they most need is love and understanding. When they cannot get them because of parental estrangement or incompetence, it is not surprising that some will look elsewhere for acceptance. Although the Internet and social networking websites provide them with one potential way of finding help or building rewarding friendships, the danger exists that they might be so desperate for such acceptance that they would even seek it from some older strangers who might want to befriend them only to satisfy perverted sexual desires.

But it would be wrong to assume that *all* youth share those same problems or would voluntarily meet—or engage in sexual activity with—an older man. Rather, only a handful of at-risk youth give rise to this problem. And even if we could find an effective way for all Internet sites to age-verify their users, many of these at-risk youth would likely still seek out acceptance from older figures using alternative means. Indeed, 79% of the victims in the study mentioned earlier were also contacted by the offenders by telephone, and almost 20% received correspondence by traditional mail. But no one would seriously consider trying to solve such a problem by age-verifying minors before they use phones or send letters.

Educators, health officials, and other organizations need to devise better strategies for assisting such at-risk youth. The first step is finding them. Again, this step is where the Internet and social networking sites actually *help* solve problems. For

example, John Draper, director of the National Suicide Prevention Lifeline,²⁹ has said that referrals from MySpace.com users have become the largest source of calls to the hotline. He says that some kids are increasingly using their social networking profiles “to in some way convey that they had suicidal intent. There is very much the potential for saving lives because the first people to hear about kids at risk are other kids.”³⁰ In fact, the organization has recently established its own MySpace profile to enable easier reporting of problems.³¹

Another independent MySpace suicide prevention site—“SOS” (Students Overcoming Suicide)—aims “to prevent and raise awareness about teenage suicide in the place where teens are most reachable; schools... Through SOS, our goal is to reach out to those in need, and offer hope to those who would otherwise have nowhere else to turn. In doing so, we want to show that nobody is truly alone in this world, no matter how bad it may seem. SOS aims to bring teens together in an attempt to unite and overcome feelings of despair, isolation, and hopelessness.”³²

Many other examples of peers assisting other at-risk peers can be found on social networking sites. On MySpace.com alone, notable examples include: “Helping Teens,”³³ “Teens Helping Teens,”³⁴ and the “Teen Support Alliance,”³⁵ all of which let youth counsel each other or suggest places where others might find help.

Teens Soliciting Teens: In this debate, much is also made of a statistic culled from the second Youth Internet Safety Survey (YISS-2) from the National Center for Missing and Exploited Children, which found that one out of every seven (13%) children has received a sexual solicitation while online.³⁶ Although this figure represents a decline from the 1-in-5 (19%) finding from the first survey (YISS-1), it’s still a disturbing number.

Importantly, however, the YISS survey noted that a significant percentage of those “solicitations” are kids talking to other kids. In other words, when 17-year old Johnny propositions 16-year-old Jenny, it counts as a “solicitation.” Of course, teens were delivering salacious solicitations to each other long before the Internet came along, but parents had no way to track sexual solicitations unless they found a dirty note in a schoolbag or pants pocket.

This reality is not to condone the rude and raunchy behavior that some teens engage in, but we need to be realistic about the issue and to understand that, in a

²⁹ www.suicidepreventionlifeline.org

³⁰ Quoted in Magid and Collier, *MySpace Unraveled*, p. 174.

³¹ www.myspace.com/suicidepreventionlifeline

³² www.myspace.com/studentsovercomingsuicide

³³ www.myspace.com/helpingteens

³⁴ www.myspace.com/whymeteenshelpingteens

³⁵ <http://groups.myspace.com/Teensupportalliance>

³⁶ Janis Wolak, Kimberly Mitchell, and David Finkelhor, *Online Victimization: Five Years Later*, National Center for Missing and Exploited Children, 2006, www.missingkids.com/en_US/publications/NC167.pdf

certain sense, this problem has always been with us. It's just more visible to us now. For the first time, we are measuring things that were previous unmeasured or unmeasurable. Regardless, teens trash-talking to other teens is a problem that will not disappear with the imposition of age-verification on social networking sites.

Parental Fears about New Technologies: Finally, it's clear that part of what is driving the push to regulate social networking sites is that many adults simply don't understand this new technology and have created a sort of "moral panic" around it.³⁷ But parents misunderstanding teens—or a new trend or technology that teens love—is really nothing new.³⁸ For example, today's grandparents will recall that when they were teenagers in the 1950s and 1960s, their parents worried about their hanging out at burger joints and roller rinks.³⁹ And today's parents will remember that in the 1970s and 1980s, their parents were concerned about their hanging around shopping malls and video arcades. Those places were the social networking sites of their eras. And so it continues with the networking sites that today's youngsters enjoy: digital, interactive websites.⁴⁰

Parents need to remember that they were once kids too, and they managed to live through many of the same fears and concerns about new media technologies and types of teen interaction. As University of North Carolina journalism professor Margaret A. Blanchard once noted:

[P]arents and grandparents who lead the efforts to cleanse today's society seem to forget that they survived alleged attacks on their morals by different media when they were children. Each generation's adults either lose faith in the ability of their young people to do the same or they become convinced that the dangers facing the new generation are much more substantial than the ones they faced as children.⁴¹

And Thomas Hine, author of *The Rise and Fall of the American Teenager*, argues: "We seem to have moved, without skipping a beat, from blaming our parents for the ills of society to blaming our children. We want them to embody virtues we only

³⁷ Wade Roush, "The Moral Panic over Social-Networking Sites," *MIT Technology Review*, August 7, 2006, www.technologyreview.com/read_article.aspx?id=17266&ch=infotech

³⁸ In the April 2006 edition of *Wired Magazine*, Tom Standage, the technology editor at *The Economist* and author of *The Victorian Internet*, highlighted some of the "moral panics" that elders of previous generations believed would consume youth culture. These included: Novels and plays, the waltz, movies, the telephone, comic books, and rock and roll music. See Tom Standage, "Those Darn Kids and Their Darn New Technology," *Wired*, April 2006, pp. 114-115.

³⁹ I borrowed this analogy from Danah Boyd of the University of California-Berkeley. See Danah Boyd, "Identity Production in a Networked Culture: Why Youth Heart MySpace," presentation before the American Association for the Advancement of Science, February 19, 2006, www.danah.org/papers/AAAS2006.html

⁴⁰ "[E]very generation of parents wishes it could eliminate all risk from children's lives. And every generation of teens engages in behaviors that make parents have that wish." Magid and Collier, *MySpace Unraveled*, p. 24.

⁴¹ Margaret A. Blanchard, "The American Urge to Censor: Freedom of Expression versus the Desire to Sanitize Society—From Anthony Comstock to 2 Live Crew," *William and Mary Law Review*, vol. 33, Spring 1992, p. 743.

rarely practice. We want them to eschew habits we've never managed to break."⁴²

Moreover, what is almost completely overlooked in the current debate over social networking is that many social networking communities have developed effective self-policing strategies. Those self-policing strategies come in both formal and informal varieties. Many online communities adopt formal policies about how to report abusive or offensive behavior. Others allow site users to tag certain content or pages as inappropriate or offensive. Site administrators can then take appropriate action, including removing troublemakers from the site or even reporting them to law enforcement authorities. Site administrators have enormous reputational incentives to self-police their own networks because most social networking sites depend on advertising revenue, and they risk losing advertisers if they don't maintain a positive standing. As Hemanshu Nigam, MySpace.com's Chief Security Office, recently told *CSO Magazine*:

The advertisers who talk to us are saying, If your site has people who are getting victimized or hit by viruses and there are dangers there, then we don't want to align our brand with yours. So there's this really cool synergy between doing safety for business reasons and doing safety because it's the right thing to do. You don't find that in many places. The [safer it is], the greater your reputation; the greater your reputation, the more advertisers feel comfortable in talking to the 135 million people who are on the site.⁴³

Equally as important are the less formal varieties of peer policing at work on many sites. Many youngsters communicate with each other about annoying or offensive users and other online threats. As noted in the preceding section, kids are more likely to respond to the positive reinforcement that comes from their peers than from adults. Again, the problem tends to be the handful of at-risk youngsters who are especially susceptible to repeated contact with and grooming by predators. If we can find ways to get other teens to identify and assist their at-risk peers, it would likely be one of the most rewarding strategies for combating this problem in the future.

This is not to say that adult supervision is unnecessary. To the contrary, adult interaction and oversight of children's online activities are essential because minors will always need a certain amount of mentoring. (Some of these mentoring strategies are discussed in the concluding section below.) But will the supervising adults be parents and educators, or will they be government officials with the power to sanction or even shut down online websites? That question is at the center of this debate.

Defining the Challenges

Before we detail some of the advantages and disadvantages associated with the leading varieties of age verification, several "big picture" questions need to be asked to

⁴² Quoted in Nancy Gibbs, "Being 13," *Time*, August 8, 2005, p. 43.

⁴³ Sarah D. Scalet, "Mr. Safety Keeps Watch on MySpace Security," *CSO Magazine*, March 2007, www.csoonline.com/read/030107/fea_myspace.html

help frame the debate:

- Everyone would agree that protecting children from potential online dangers is important, but so too is protecting the privacy and relative autonomy of children. And minors have speech rights too.⁴⁴ In this debate, there will be a great deal of tension between these competing values. **How much privacy and freedom of expression and association will need to be sacrificed in an attempt to provide greater online security?** How do we balance the constitutional / First Amendment-related values at stake here—for both adults and children? Are we treating minors as guilty until proven innocent by making it so difficult for them to communicate with others in online communities?
- The Internet is a global platform, and social networking is a worldwide phenomenon. Will domestic solutions “scale” for globally available networks? Should they? More important, **will domestic regulatory solutions hurt mainstream social networking sites and drive youngsters offshore to the truly dark alleys of the Internet**, which are beyond the reach of domestic laws? As Ernie Allen, President of the National Center for Missing and Exploited Children asks, “We can make these things absolutely safe and secure, but do we then drive people into offshore versions of this that are beyond regulation?”⁴⁵
- **How broadly will “social networking sites” be defined?** Will chat rooms, hobbyist sites, instant messaging, video sharing sites, online marketplaces or online multiplayer gaming sites qualify?⁴⁶ If so, how will they be policed and how burdensome will regulation become for smaller sites? Does the government have the resources to engage in such policing activities when almost all websites now have a social networking component?⁴⁷
- **Are we devising solutions that unjustly penalize the online world relative to the offline world?** Will new rules or regulations single out online social networking sites for differential treatment relative to offline social networking sites? After all, shopping malls and public parks are social networking sites too. Will kids be age-verified there as well?

⁴⁴ See “CDT Calls on Senate to Reject the ‘Deleting Online Predators Act,’” Center for Democracy and Technology *Press Release*, August 4, 2006,

www.cdt.org/speech/20060811dopa.pdf. CDT notes that “the vast bulk of the speech blocked by DOPA—teens chatting with their friends, posting photos and linking to their favorite music—is perfectly healthy (or at least harmless), and is *completely* legal.”

⁴⁵ Sarah D. Scalet, “Mr. Safety Keeps Watch on MySpace Security,” *CSO Magazine*, March 2007, www.csoonline.com/read/030107/fea_myspace.html

⁴⁶ Matt Slagle, “Social Networking Comes to Casual Games,” *USA Today*, September 7, 2006.

⁴⁷ For example, in March 2007, *USA Today* announced a major redesign of its USAToday.com website that recast the site as a social networking community. The site redesign featured a variety of new tools to make the site more interactive, including the ability for users to set up their own profiles, upload photos, write blogs, and send messages to other users. This change illustrates how difficult it will be for lawmakers to define social networking sites in the future. See [www.usatoday.com/news/community-features.htm](http://www.usatoday.com/news/community/features.htm)

- **Will increased online policing divert resources from offline policing?** Stated differently, because physical harm to children occurs only through real-world encounters, will a focus on the online component come at the expense of offline policing of real-world harms?

With such questions helping to frame the debate, we turn now to specific concerns or challenges associated with various age verification proposals.

The Complexities of Human Identification

Generally speaking, the problem that age verification is supposed to solve is to keep older people away from youngsters, at least in certain circumstances. Also, some proponents wish to use age verification to ban preteen access to social networking sites. To accomplish either of those objectives, we must be able to effectively verify everyone's age by consulting reliable records about those looking to create an account on a social networking site. In other words, when Janie Smith comes to a social networking site for the first time, the site must be able to verify not only that she is Janie Smith, but that she really is as old as she claims to be. But this verification is easier said than done.

Consider first what is required to verify an *adult's* identity. When government officials or even corporations seek to verify someone identify or age, they can rely on birth certificates, Social Security numbers, driver's licenses, military records, home mortgages, car loans, other credit records, or credit cards.

But even with all those pieces of information, challenges remain. Is the information publicly accessible or restricted by legal or other means? Are all the underlying pieces of information and documentation trustworthy, or have they been manipulated or misrepresented in some way? Has someone faked his or her identity? And so on. Thus, while the identity authentication systems—both public and private—have improved significantly in recent decades, they still face some inherent challenges and concerns about fraud.⁴⁸

The current concern about “identity theft” demonstrates the complexities and level of difficulty involved in stamping out this problem. Even U.S. passports, which are relatively robust identification documents that contain authentication data, are occasionally forged with success. “It is safe to assume that future age verification efforts will yield failures on par with other identification/authentication mechanisms,” says information security expert Jeff Schmidt, CEO of Authis, Inc.⁴⁹ “When one considers how frequently college students successfully circumvent age verification requirements in person and with government issued documents, one can begin to grasp the challenges that lie ahead.”⁵⁰

⁴⁸ For a comprehensive discussion of such matters, see Jim Harper, *Identity Crisis: How Identification Is Overused and Misunderstood* (Washington, D.C.: Cato Institute, 2006).

⁴⁹ Jeff Schmidt, e-mail conversation on file with author, February 19, 2007.

⁵⁰ Ibid.

Importantly, we're talking just about adults here. When the focus of identity verification efforts shifts to minors, the endeavor becomes far more complicated. Minors don't have home mortgages or car loans. They don't have military records and most have never worked. Most don't have driver's licenses or credit cards either.

Of course, minors do have birth certificates, Social Security numbers, and school records, but both parents and government officials have long demanded that access to those records be tightly guarded. That's for a very good reason: As a society, we take privacy seriously—especially the privacy of our children. Laws and regulations have been implemented that shield such records from public use, including the Family Educational Rights and Privacy Act of 1974 and various state statutes.⁵¹

Also, to the extent that age verification of adults works for some websites—online dating services, for example—it is important to realize that in most of those cases *the users want to be verified*. In that context, identity authentication increases marketability of a user's "profile," or it allows him or her to participate more actively in an environment where trust is essential. This fact makes it far more likely that age verification will work because user compliance is driven by market forces, not regulation. That compliance will not be the case when users—especially kids—inherently resist the idea of being age-verified before they go onto certain websites. (We should also not forget that some kids will share their online credentials or passwords with friends.)

It is also important to realize that age verification and background checks are not synonymous. Information security expert John J. Cardillo, President and CEO of Sentinel, a leading authentication firm, argues that:

Most people are ignorant of what we do. They hear the words "check" or "verification" and they assume a full background check will be run on the individual. When this is sponsored by an AG, the chief law enforcement officer of their state, there's a perception that the criminal background checks are inclusive in whatever they're proposing. 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.⁵²

Again, this points to the danger of creating a false sense of security online by mandating a solution that doesn't address the real problem.

⁵¹ www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

⁵² John J. Cardillo, e-mail conversation on file with author, March 11, 2007.

Finally, the special challenges raised by the nature of the Internet and online communication must be reiterated. Finding a dependable source of identity or age information and then reliably matching it to someone thousands of miles away on the Internet (perhaps in another jurisdiction, or even another country) is a daunting challenge—made even more difficult by the fact that a remote individual may be actively attempting to subvert the age verification process. Solving this problem necessitates authentication data that are appropriate for online interaction. In the real world, we perform in-person authentication with a photo or physical description; the online world requires a username/password combination, biometric authenticator, or physical security token. An arms-race scenario is obviously at work here, and because a perfect solution is impossible, we must guard against a false sense of security. Lastly, because technology is evolving at such a rapid pace in this area, there is a risk that legislative solutions will become obsolete very rapidly.

In light of those complications, how would government, social networking sites, or anyone else, go about age-verifying minors online?

National ID Cards for Kids?

In the extreme, government could demand that all minors be issued the equivalent of a domestic passport or a national ID card. After all, minors aged 14 to 17 are already required to obtain a passport before they travel overseas.⁵³ Minors under 14 must have both parents or legal guardians appear together to vouch for the child when applying for a passport. Conceivably, government could simply extend this model to incorporate a domestic identification requirement. Once the youngster had been issued such a domestic passport, it could be requested by others—including social networking sites—as proof of age. Sites could cross-reference a government national ID database to verify identity.

Clearly, however, imposing such a solution domestically would raise serious privacy concerns because it would require the collection, retention and processing of sensitive information about children. Adults are not required to carry such a domestic passport or national ID card, so why should children? Indeed, all the same privacy concerns related to national ID cards for adults would be amplified with children because, as a society, we generally take extra precautions to protect the privacy of minors and their personal information. And a national ID card for kids would need to include a great deal of information about themselves to allow the card to be used by third parties online as an age-verifying tool. Government would need to issue an age-verified identity, user name, and password to every child.

Particularly concerning is the fact that a national ID card for children would require the creation of more government databases and bureaucracy. The potential for “mission creep” then enters the picture in that more tracking of children by government (and others) becomes possible. What other uses might there be for such information?

⁵³ U.S. Department of State, “How to Apply in Person for a Passport,” http://travel.state.gov/passport/get/first/first_830.html

We don't know, and we probably don't want to find out.

The costs of setting up and enforcing such a system would be substantial and must also be considered. Although the cost of digital storage continues to fall, we're talking about potentially massive digital databases here. But the more important cost factor is the human time and effort that would go into collecting, processing, and organizing such records and databases.

For those reasons, a government-issued ID card or age verification scheme for kids is a nonstarter. It would raise grave privacy concerns, induce public paranoia, probably encourage a great deal of evasion, and require significant government expenditure to enforce. Moreover, a national ID card would do little to prevent youngsters from visiting offshore sites.

Sources of Age Information

Thus, if social networking sites are going to age-verify minors, they will likely need to devise or rely on some other, nongovernmental solution. The most commonly proposed solutions typically fall into the following groupings:

- (1) Credit cards as approximate age proxies;
- (2) Driver's licenses as approximate age proxies or as a source of date of birth;
- (3) Birth certificates as a source of actual date of birth;
- (4) Parents or guardians vouching for minors;
- (5) Schools vouching for minors;
- (6) Third parties vouching for minors; and,
- (7) Biological or biometric determination of age.

The advantages and disadvantages associated with each approach will be discussed briefly.

(1) Credit Cards as Approximate Age Proxies: Credit cards are often viewed by policy makers as the silver bullet solution for age verification. Even though credit card companies typically do not wish their cards to be used as age verification tools, government has advocated their use in that way in the past. But they are not a silver bullet.

"Mere possession of a credit card is not a reliable assertion of identity or age," argues Jeff Schmidt of Authis.⁵⁴ Credit cards can be a rough proxy for age on the assumption that only adults over the age of 18 have credit cards, but that assumption is false. Many minors are given credit cards by their parents. Youngsters can borrow or steal credit cards from their parents or others. And Schmidt notes that newly created stored value cards, specifically marketed for use by children, "are in many cases indistinguishable from actual credit cards—both in physical appearance and in the back-

⁵⁴ Jeff Schmidt, e-mail conversation on file with author, February 19, 2007.

end transaction processing systems.”⁵⁵ Sentinel’s John Cardillo points out additional reasons why credit cards are not effective age verification tools:

When a card is used for verification purposes, an authorization on that card is run for \$1.00 (or less), however a charge isn’t put through. The card typically isn’t reconciled against any database for name and/or age, nor is a signature checked. Because of the insignificant dollar amount, the only thing that’s checked for security purposes, in some instances, is zip code. Anyone who’s ever bought gasoline with a credit card knows this to be true. Our names and ages aren’t checked at the pump. Check your statement online next time you gas up. You’ll see an authorization for \$1.00 and the actual charge a few days later. The same merchant banks handle the transactions online. In other words, in most cases, all that’s being verified is that the card account isn’t closed or stolen. Who’s using it is irrelevant.⁵⁶

Moreover, “many parents may feel uncomfortable giving their credit card number online at children’s Web sites where there is no [commercial] transaction involved,”⁵⁷ notes a coalition of major commercial organizations, including the American Advertising Federation, American Association of Advertising Agencies, Association of National Advertisers, The Direct Marketing Association, Inc., and Magazine Publishers of America. In a June 2005 filing to the Federal Trade Commission, those organizations noted that “in light of current online scams, heightened concerns about online security, and the rise of such practices as phishing, parents may be reluctant to provide credit card numbers absent a transaction.”⁵⁸ But that begs the question: If lawmakers require social networking sites to process a financial transaction to age-verify, is that fair? In particular, is it fair for low-income families? And what about those families that do not possess a credit card?

Finally, the law is not even settled about using credit cards for access to adult-oriented websites. The Child Online Protection Act (COPA) was passed by Congress in 1998 in an effort to restrict minors’ access to adult-oriented websites. The measure provided an affirmative defense to prosecution if a website operator could show that it had made a good faith effort to restrict site access by requiring a credit card, adult personal identification number, or some other type of age-verifying certificate or technology. But the legislation was immediately challenged and has gone to the Supreme Court for review *twice*. And the law is still being debated in a lower court. Thus, almost 10 years after its initial passage, the legislation remains stuck in jurisprudential limbo after endless legal wrangling about its constitutionality.

Incidentally, COPA established an expert Commission on Online Child Protection to study methods for reducing access by minors to harmful material on the

⁵⁵ Jeff Schmidt, e-mail conversation on file with author, February 19, 2007.

⁵⁶ John J. Cardillo, e-mail conversation on file with author, March 11, 2007.

⁵⁷ American Advertising Federation, American Association of Advertising Agencies, Association of National Advertisers, The Direct Marketing Association, Inc., and Magazine Publishers of America, Filing in COPPA Rule Review 2005, June 27, 2005, p. 5.

⁵⁸ *Ibid.*

Internet. As part of its final report, the COPA commission said that credit card-based age verification would be completely inappropriate for instant messaging and chat, which were the precursors of social networking. The commission found: "This system's limitations include the fact that some children have access to credit cards, and it is unclear how this system would apply to sites outside the U.S. It is not effective at blocking access to chat, newsgroups, or instant messaging."⁵⁹

(2) Driver's Licenses as Approximate Age Proxies or as a Source of Actual Date of Birth: Driver's licenses are occasionally mentioned in this debate as a possible age verification tool. But driver's licenses have some rather obvious limitations. First, driver's licenses are generally not granted to minors under 16. Second, although 16 is the average age that a minor can get a license in most states, requirements vary by state. Third, many minors don't bother getting a driver's license. Finally, unlike when someone presents a driver's license to prove his or her age in public places or private establishments, a website cannot physically see the person who is asking to be verified. Thus, the website operator would have to run the driver's license number against a publicly accessible database, which would raise privacy concerns.

Additionally, the Driver's Privacy Protection Act of 1994 generally prohibits states from disclosing personal information that their drivers submit to obtain a license.⁶⁰ Sentinel's John Cardillo points out that only 25 states currently allow dissemination of their driver's license records, meaning that half of the states wouldn't be able to comply with an online age verification mandate involving driver's licenses. For those reasons, driver's licenses are just as impractical as credits cards for age-verifying minors online.

(3) Birth Certificates as a Source of Actual Date of Birth: Birth certificates are a reliable source of date of birth and have been nearly universally issued for at least the past 50 years. But, as Jeff Schmidt points out, "there are at least 1,000 entities within the U.S. that issue birth certificates [and] they are extremely inconsistent and subject to forgery. Also, they do not contain any useful authentication information and as purely paper documents translate poorly into the online world. Birth certificate issuance and reliability outside of the U.S. are inconsistent at best."⁶¹

Moreover, it would extremely time-consuming and costly for parents and site administrators to be exchanging hard copies of birth certificates by mail, which is presumably the way the system would work. It could take days, even weeks, to complete the process. In the meantime, kids would probably look to go online elsewhere. For these reasons, birth certificates are of little use as an online age verification tool.

(4) Schools Vouching for Minors: Schools have more information about our

⁵⁹ Commission on Online Child Protection, Final Report, October 20, 2000, www.copacommission.org/report/ageverification.shtml. Also see Computer Science and Telecommunications Board, National Research Council, *Youth, Pornography, and the Internet*, (Washington, D.C.: National Academy Press, 2002, pp. 206-209, 339-349.

⁶⁰ www.privacilla.org/government/dppa.html

⁶¹ Jeff Schmidt, e-mail conversation on file with author, February 19, 2007.

children than probably every other institution or organization combined. They have very detailed records about kids, their ages and much more, which makes schools a logical candidate for participation in a possible age verification system for minors. But involving schools in any age verification scheme would raise serious privacy concerns and administrative problems.

Depending on how the scheme worked, the administrative burdens imposed on schools could be significant. Someone at each school would have to be in charge of answering phone calls and e-mails from potentially hundreds of website operators looking to age-verify minors. Who will be liable if things go wrong? The school? The school district? An employee in the school's administrative department who accidentally releases thousands of digital records? And will schools receive the additional funding needed to administer whatever scheme is mandated?

Moreover, if schools are required to create more accessible databases containing personal information about minors, who else besides social networking websites would be given access? Data breaches would become a real concern for both students and schools alike. Once again, such a scheme would run up against federal or state laws. For example, the Family Education Rights and Privacy Act of 1974 makes it illegal to release school records without written permission from parents.⁶²

However, schools actually produce some publicly available information about children that does not contain sensitive personal information. For example, schools publish yearbooks containing the names and pictures of each child in the school by grade. That information could be extraordinarily helpful to someone seeking to age-verify minors. And it would have the added benefit of avoiding many privacy concerns about accessing a school's private databases containing private information about minors.

But who would go about collecting such less-sensitive, publicly available information about minors? The collection of that information could be time-consuming and costly. Nonetheless, it might be possible for parents, parent groups, or other organizations to tap that information in an attempt to help age-verify children. This possibility is discussed next.

(5) Parents or Guardians Vouching for Minors: A new bill was recently introduced in Georgia that would make it illegal for a minor to maintain an account or webpage on a social networking site "without the permission of the minor's parent or guardian and without providing such parent or guardian access to such profile web page."⁶³ Similar measures were recently introduced in North Carolina⁶⁴ and Connecticut⁶⁵ that would require social networking sites not only to obtain parental approval but also take steps

⁶² www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

⁶³ www.legis.ga.gov/legis/2007_08/fulltext/sb59.htm

⁶⁴ www.ncleg.net/Sessions/2007/Bills/Senate/HTML/S132v0.html

⁶⁵ Susan Haigh, "Conn. Bill Would Force MySpace Age Check," *Yahoo News.com*, March 7, 2007, http://news.yahoo.com/s/ap/20070307/ap_on_hi_te/myspace_dangers;_ylt=At1jsr5xeFgo76tZi6i.fm1j24c
A

to verify that they are the actual parents of the child.

This approach will appeal to many because it can be likened to a parent signing a “permission slip” for a child. Unfortunately, parental permission-based approaches are more complicated for online activities. Because websites are far away from the parents, how is the site operator going to ensure that the person vouching for the child’s age is really the parent or even an adult? Would the verifier mail or fax notarized documents? Those documents can be forged, of course. Mandatory follow-up phone calls would be cumbersome, costly, and potentially viewed as intrusive. And the use of credit cards to satisfy the permission requirement might raise some of the same problems already discussed above.

Despite these potential drawbacks, this was the general framework established by the Children’s Online Privacy Protection Act (COPPA) of 1998, which required websites that marketed to children under the age of 13 to get “verifiable parental consent” before allowing children access to their sites. The Federal Trade Commission (FTC), which is responsible for enforcing COPPA, adopted a sliding scale approach to obtaining parental consent.⁶⁶ The sliding scale approach allows website operators to use a mix of the methods mentioned above to comply with the law, including print-and-fax forms, follow-up phone calls and e-mails, and credit card authorizations. The FTC also authorized four “safe harbor” programs operated by private companies that help website operators comply with COPPA.⁶⁷

In a recent report to Congress, the FTC said that no changes to COPPA were necessary at this time because it had “been effective in helping to protect the privacy and safety of young children online.”⁶⁸ In discussing the effectiveness of the parental consent methods, however, the agency also said that “none of these mechanisms is foolproof” and that “age verification technologies have not kept pace with other developments, and are not currently available as a substitute for other screening mechanisms.”⁶⁹ This seems to imply that the FTC does not regard COPPA’s parental consent methods as the equivalent of perfect age verification.

And the marketplace experience with COPPA so far reflects that conclusion. One of the problems associated with the current COPPA regime is that “Children quickly learned to lie about their age in order to gain access to the interactive features on their favorite sites,” notes Denise G. Tayloe, CEO of Privo, Inc., one of the four FTC-approved safe harbor programs.⁷⁰ “As a result, databases have become tainted with

⁶⁶ See: Federal Trade Commission, *How to Comply with The Children’s Online Privacy Protection Rule*, November 1999, www.ftc.gov/bcp/online/pubs/buspubs/coppa.htm

⁶⁷ The four safe harbor programs are administered by the Children’s Advertising Review Unit of the Council of Better Business Bureaus (“CARU”); the Entertainment Software Rating Board (ESRB); TRUSTe; and Privo.

⁶⁸ Federal Trade Commission, *Implementing the Children’s Online Privacy Protection Act: A Report to Congress*, February 2007, p. 1, www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf

⁶⁹ *Ibid.*, p. 12-13.

⁷⁰ Denise Tayloe, “It’s Time to Comply with COPPA,” *The Privacy Advisor*, vol. 6, no. 10, October 2006, p. 5.

inaccurate information and chaos seems to be king where COPPA is concerned,” she says.⁷¹ Parry Aftab of Wired Safety confirms this, noting that: “Preteens quickly learned that if they say they are under thirteen they will be prohibited from using many sites. So they regularly lie about their age everywhere online.”⁷²

Despite these flaws, Tayloe argues that COPPA serves an important role. Even though “there is no perfect solution” and it is not possible to completely “stop a child from lying and putting themselves at risk,” Tayloe believes that the law “provides a platform to educate parents and kids about privacy.”⁷³ Of course, providing a platform to educate parents and kids about online privacy or safety is very important, but it is not necessarily synonymous with strict age verification.

Nonetheless, these permission-based verification schemes might work reasonably well for smaller, closed online communities in which the kids and parents are willing to take the time (and expense) to undertake extensive authentication. For example, smaller social networking sites such as ZoeyRoom.com, Imbee.com, ClubPenguin.com, and Tweenland.com have extremely strict enlistment policies, primarily because they target or allow younger users. As Sue Shellenbarger of the *Wall Street Journal* explains:

The under-16 sites pose few of the hazards linked to networking sites for older people. The activities range from chats and blogging to creating virtual pets or characters and acting out roles in virtual cities. For a child to register, the sites typically require a parent’s email permission, a parental signature on a permission form, or a parent’s credit card verification. Some limit young children’s interchanges to drop down menus of preapproved words and phrases. Most filter content for inappropriate material and employ live adult monitors who ensure that kids’ conversations don’t stray off course. Some limit chats or blog access to participants who are already preapproved and already known to a child’s family.⁷⁴

Ironically, one can probably safely assume that the kids using such services are not in the high-risk group discussed earlier. The parents who use such services are probably doing a fine job of mentoring their kids and don’t really need to resort to such restrictive solutions. Nonetheless, such highly restrictive “walled garden” approaches do provide parents with greater ease of mind. That’s not necessarily because of the strict enlistment policies so much as the extreme limitations on what kids can do on those sites or with whom they can communicate while online.

But regardless of how well the above-mentioned parental consent schemes work in practice for these smaller, more closed online communities—and some experts do

⁷¹ Tayloe, *Ibid.*

⁷² Parry Aftab, Filing in COPPA Rule Review 2005, June 27, 2005, p. 5, www.ftc.gov/os/comments/COPPARulereview/516296-00021.pdf

⁷³ Denise Tayloe, e-mail conversation on file with author, March 15, 2007.

⁷⁴ Sue Shellenbarger, “How Young is Too Young When a Child Wants to Join the MySpace Set?” *Wall Street Journal*, October 19, 2006, p. D1.

question how well they actually work⁷⁵—such solutions lack scalability. Schemes that demand laborious and expensive enrollment requirements, or that greatly limit functionality and interactivity after users sign up, will almost certainly not work for larger social networking sites with a massive community of users. The administrative burdens would be significant for both site operators and parents alike. For example, Parry Aftab notes that COPPA has made it much more difficult for some smaller website operators to staff afloat. “The cost of obtaining verifiable parental consent for interactive communications is very high, estimated at more than \$45 per child, and even at that price [consent is] difficult to obtain.”⁷⁶

And because users would sacrifice a great deal of autonomy and functionality once online, many would likely rebel against the system or would seek to subvert it in some fashion. If such a system significantly slows or impedes the creation of new accounts for domestic social networking sites, it will create a perverse incentive for kids to seek other sites with less-restrictive policies, including offshore sites.

One can imagine other ways that parents could work together and use publicly available information about kids to credential them before they go online. But the scalability of those solutions will always likely limit their effectiveness.

(6) Third Parties Vouching for Minors: Third-party vouching is a variation of the scenario just described above. Instead of having parents vouch for children, a third party would do so. It might be possible for respected organizations (e.g., civic or religious organizations, etc) in local communities to play a role in the age verification process. In the extreme, local law enforcement officials might be the third parties.

But this approach would suffer some of the same downsides as the plans discussed earlier. In addition, it would add a layer of discomfort or uncertainty to the process because those doing the verifying would not be as trusted as parents or schools. And would there need to be some sort of certification process for the age certifiers? If there weren't, that might raise some privacy concerns because those being

⁷⁵ Internet security expert Cardillo argues that even these sites and schemes are vulnerable:

During an analysis of the security processes of certain sites we tested Imbee's. Our security team was able to create several fake children. More troubling was the inconsistency of the information used to do so. We used a fake name for the parent, a different fake name created for the Yahoo! e-mail account used at registration, and my credit card info (because the name on the CC is irrelevant). Fictional child, and three fake identifiers on supposedly the same adult. Not one red flag was raised, and we were allowed onto the site without a problem. Our team was able to do this multiple times. Had we been a real bad guy, we could have, at any time, chatted with other kids on the site as a child. One of several different children actually. Not only isn't it a security solution, it's downright dangerous.

Thus, the real bad guys out there intent on doing harm to children might still be able to exploit this sort of process. Because many predators have children of their own, they might use this approach to obtain an ID for their own kids and then go online under their child's name to prey on other children. But because they are “verified,” a false sense of security now exists. Again, this is a major problem.

⁷⁶Parry Aftab, Filing in COPPA Rule Review 2005, June 27, 2005, p. 2, www.ftc.gov/os/comments/COPPArulereview/516296-00021.pdf

forced to be age-verified might not trust the third parties with their personal information.

(7) Biological or Biometric Determination of Age: Biological or biometric identifiers rely on some intrinsic human attribute (e.g., fingerprints or retinal scans) to verify someone's identity. The problem with using biological or biometric identifiers for Internet websites is that they would work only if coupled with age information in some sort of database. For example, some laptop computers use a fingerprint reader to verify that the user is authorized to use the machine. But the fingerprint scan tells the machine nothing about the age of that user. The same would be true of a retinal scan.

Some serious dangers are associated with using biometric authentication methods as well. If a user loses an identification card or forgets a personal identification number or password—or if these things are stolen or compromised in any way—they can always be replaced. Not so with a fingerprint or retinal pattern. They are yours for life; if they are compromised, the results could be disastrous.

In the future, biometric authentication devices may be developed that will avoid such problems. For example, i-Mature is a new biometric device that measures the size and structure of the bones in human fingers to gauge a person's age. Because a child's finger contains more cartilage than solid bone, the i-Mature device can measure how developed the bone is and then can generally predict the age of the child.⁷⁷

The great advantage of that device is that no personal information about the youngster needs to be collected. But although the device is capable of *approximately* gauging a child's age, it is not a precise instrument. It cannot tell us if a child is exactly 14 or 18 years old, which is obviously important for purposes of this debate. And what about children whose bones are physically underdeveloped for their ages? They might be unfairly penalized by the device.⁷⁸

Moreover, even if we accepted those limitations, it is unrealistic to think such a device has any chance of being ubiquitously deployed and widely used. To be effective, it would require a vast infrastructure of devices to be deployed to every home. That's not going to happen. And there is always the chance that someone might develop a "fake finger" to fool the device and then start marketing it online. History has shown that no technology is foolproof.

Finally, we must not be forget that some child predators have children of their own and could defeat the device by forcing their children to use it so they could go online as an "age-verified" child. Again, this would give rise to a false sense of security online.

⁷⁷ www.biometricwatch.com/BW_in_print/age_group_recognition.htm and www.netcaucus.org/books/childsafety2006/i-mature.pdf

⁷⁸ Hiawatha Bray, "Putting a Finger on a Person's Age," *Boston Globe*, February 14, 2005, www.boston.com/business/technology/biotechnology/articles/2005/02/14/putting_a_finger_on_a_persons_age/

No Single, Simple Solution

In sum, the question of how to age-verify minors has no easy solutions. As Kim Cameron, who holds the title “Architect of Identity” for the Microsoft Corporation, argues:

the emergence of a *single simplistic digital identity solution* as a universal panacea is not realistic. Even if some miracle occurred and the various players could work out some kind of broad cross-sector agreement about what constitutes perfection in one country, the probability of extending that universally across international borders would be zero. [emphasis in original].⁷⁹

To the extent that a workable technical solution can be found, it will likely entail a combination of elements from several of the approaches discussed here plus something else not yet envisioned or invented. And for the reasons Cameron points to, it is unlikely it will be highly centralized or unified. Indeed, we could see several solutions developing on several different levels. Some websites might unify around an extremely restrictive solution that demands multiple layers of authentication. Others might settle for something far less restrictive. Market forces will create sites in each of those categories—if there is demand.

Regardless, whenever solutions are proposed, tough questions must be asked about how the system would work and whether or not making it work is cost-effective. In particular, it is essential to scrutinize proposed solutions to ensure the following:

- **They do not result in unintended consequences or solutions that don’t solve the problems they were intended to address;**
- **They do not create a false sense of security that might encourage some youngsters (or adults) to let their guard down; and**
- **They do not create potential incentives to push mainstream social networking sites offshore.** To reiterate, however bad parents or policy makers think social networking sites are today—and, in reality, the sites are not nearly as bad as they imagine—those sites are infinitely superior to potentially shady offshore websites that are completely unaccountable to U.S. officials. And the domestic sites are more accountable to the general public and are responsive to press scrutiny.

Focus on Education First

In the meantime, *it is vital that the search for technical solutions not divert attention from the truly important task of educating both parents and children about*

⁷⁹ Kim Cameron, *The Laws of Identity*, May 12, 2005, www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

online safety. Whereas workable age verification solutions could take years to emerge—and there is no guarantee of their long-term effectiveness—basic Internet safety education can begin *today*. And everyone—government, social networking sites, and parents—has a role to play.

(a) The Role of Government / Educators: In 2002, the National Research Council of the National Academy of Sciences convened a blue-ribbon panel of experts to study how best to protect children in our new Internet world. Under the leadership of former U.S. Attorney General Richard Thornburgh, the group produced a massive report that recommended a mix of efforts to accomplish that task. The report discussed a sweeping array of methods and technological controls for dealing with potentially objectionable media content and online troublemakers. Ultimately, however, the experts used a compelling metaphor to explain why education was the most important tool on which parents and policy makers should rely:

Technology—in the form of fences around pools, pool alarms, and locks—can help protect children from drowning in swimming pools. However, teaching a child to swim—and when to avoid pools—is a far safer approach than relying on locks, fences, and alarms to prevent him or her from drowning. Does this mean that parents should not buy fences, alarms, or locks? Of course not—because they do provide some benefit. But parents cannot rely exclusively on those devices to keep their children safe from drowning, and most parents recognize that a child who knows how to swim is less likely to be harmed than one who does not. Furthermore, teaching a child to swim and to exercise good judgment about bodies of water to avoid has applicability and relevance far beyond swimming pools—as any parent who takes a child to the beach can testify.⁸⁰

The Thornburgh Commission got it right: There is simply no substitute for education. Regrettably, we are clearly failing to teach our children how to swim in the new media waters today. Indeed, to extend the metaphor, it is as if we are generally adopting an approach that is more akin to just throwing kids in the deep end and waiting to see what happens.

The way to rectify this situation is to significantly step up media literacy plans and online safety educational campaigns in America. Media literacy programs teach children and adults alike to think critically about media to better analyze and understand the messages that media providers are communicating.⁸¹ Media literacy and online safety lessons should be pushed by government at every level of education.⁸² And those efforts should be accompanied by public awareness campaigns to better inform parents about the parental control tools at their disposal. Lawmakers and educators need to

⁸⁰ Computer Science and Telecommunications Board, National Research Council, *Youth, Pornography, and the Internet* (Washington, D.C.: National Academy Press, 2002), p. 187.

⁸¹ Marjorie Heins and Christina Cho, "Media Literacy: An Alternative to Censorship," Free Expression Policy Project, 2003, www.fepproject.org/policyreports/medialiteracy.html

⁸² Elizabeth Thoman and Tessa Jolls, "Literacy for the 21st Century: An Overview & Orientation Guide to Media Literacy Education," Center for Media Literacy, 2005, p. 10, www.medialit.org/reading_room/article540.html

focus on finding the “teachable moments” in the educational process when we can instill online safety lessons into our children and can constantly reinforce those lessons over time.

Currently, however, government efforts to promote awareness have been diffuse and largely uncoordinated among various agencies and programs. One notable exception at the federal level has been the OnGuardOnline.gov website, which “provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.”⁸³ Six federal agencies collaborated to create the website.⁸⁴ Although the initiative doesn’t focus exclusively on parental controls or online child protection, it does offer some helpful tips on that front. The site includes a section on social networking sites with “A Parent’s Guide” to help them keep kids safe online.⁸⁵

If government officials want to encourage more widespread awareness and adoption of parental control tools and online child safety methods, Rep. Melissa Bean (D-IL) has proposed legislation to better coordinate and expand online safety efforts and education. Her bill, H.R. 1008, the “Safeguarding America’s Families by Enhancing and Reorganizing New and Efficient Technologies Act of 2006,” or “SAFER NET” Act, would do the following:⁸⁶

- Create a new Office of Internet Safety and Public Awareness at the FTC that is explicitly responsible for improving public awareness and education about Internet safety. This office would be the primary federal contact on Internet safety, serving as a resource and clearinghouse for consumers, the industry, and other Internet safety initiatives. It would also work with other entities (federal, state, local, private) to reduce redundancy and to promote best practices for promoting and ensuring internet safety. The office would also report to Congress annually on the state of internet safety, emerging threats, and the costs to the economy.
- Launch a national public awareness campaign to educate Americans about online threats and about how to best protect themselves and their families from being the victims of online predators, financial schemes, ID theft, and more.
- Authorize federal grants to support efforts to promote Internet safety conducted by qualifying entities such as schools, nonprofit organizations, state and local governments, law enforcement agencies, and businesses.

⁸³ <http://onguardonline.gov/index.html>

⁸⁴ They are the Federal Trade Commission, the Department of Commerce, the Securities and Exchange Commission, the U.S. Postal Inspection Service, the Office of Justice Programs, and the Department of Homeland Security.

⁸⁵ <http://onguardonline.gov/socialnetworking.html>

⁸⁶ “Bean Introduces Legislation to Fight Child Predators and Combat Cyber-Crime,” Office of Congresswoman Melissa Bean, *Press Release*, February 13, 2007, www.house.gov/apps/list/press/il08_bean/2132007_SAFER_NET_Act.html

The bill represents an admirable attempt to better coordinate and expand Internet safety education. Rep. Bean deserves credit for taking her message “on the road” by hosting an ongoing series of town hall meetings in her district to discuss online safety with her constituents. Presumably, if the legislation she introduced were ever implemented, the new FTC Office of Internet Safety and Public Awareness could create briefing plans and materials for other lawmakers who want emulate Rep. Bean’s efforts to educate constituents. Officials from that office might be available to assist lawmakers or even accompany them on town hall speaking tours to discuss parental controls and online child safety.⁸⁷

State and local governments could do more too. In September 2006, the Commonwealth of Virginia produced an outstanding report titled “Guidelines and Resources for Internet Safety in Schools” that can serve as model legislation for other states in this regard.⁸⁸ State and local officials need to follow the roadmap outlined by Virginia and begin integrating media literacy and Internet safety lessons into educational curricula at every level.⁸⁹ Librarians need to be trained to play a role too. And funding needs to be provided for all those efforts.

(b) The Role of Social Networking Websites: Social networking website operators must step up to the plate with better tools and information to combat online risks. Some sites already use crude methods to check whether kids are being honest about their ages. More important, as mentioned previously, those sites monitor activities within their online communities to weed out suspicious or troubling behavior. Almost all mainstream sites offer clearly labeled buttons and links on their home page, thus allowing users to report abuse or inappropriate material or to find online safety tips.⁹⁰ Those sites also allow users to hide personal information and some sites even allow users to see the usernames of individuals who have viewed whatever information users decide to make publicly available on their pages and profiles.

Some sites go further. New social networking sites for teens such as NickTropolis.com⁹¹ and Habbo.com⁹² illustrate how safety and security are becoming an essential part of attracting users and gaining the trust of parents. NickTropolis lays out clear ground rules for its users and offers an online safety guide for teens and safety

⁸⁷ Such an education-based approach has the added benefit of remaining within the boundaries of the Constitution and the First Amendment because government would not be seeking to restrict speech, but simply to better inform and empower parents regarding the parental control tools and techniques already at their disposal. The courts have shown themselves to be amenable to such educational efforts compared to regulatory enactments.

⁸⁸ www.doe.virginia.gov/VDOE/Technology/OET/internet-safety-guidelines-resources.pdf

⁸⁹ The text of the enabling legislation can be found at: <http://leg1.state.va.us/cgi-bin/legp504.exe?061+ful+HB58ER>

⁹⁰ For example, for Xanga.com see: www.xanga.com/ReportContent.aspx and for Microsoft’s Windows Live Spaces see: http://support.live.com/eform.aspx?productKey=wspacesabuse&page=wlsupport_home_options_form_byemail&ct=eformts

⁹¹ www.nicktropolis.com

⁹² www.habbo.com

information for parents.⁹³ Habbo recently designated February as “Teen Online Safety Awareness Month” and began running special promotions and interactive activities to heighten online safety awareness for both the 2 million teens that use the site and their parents.⁹⁴ Habbo’s home page also contains links to a very detailed “Parent Online Safety Guide”⁹⁵ as well as a “Parent Toolbox.”⁹⁶ The site has partnered with *Teen Magazine* to increase the visibility of the effort.

MySpace.com recently announced that it would soon make sophisticated monitoring software available to parents that will allow them to keep better tabs on their kids’ online interactions. The software, dubbed “Zephyr,” will let parents see the name, age, and location that children are listing on their MySpace accounts. It would update parents if their children changed that information for any reason. For privacy reasons, however, the software will not let parents read their child’s personal e-mail.⁹⁷ The company has also sponsored public service announcements about online safety featuring actor Kiefer Sutherland of the popular Fox television drama “24.”⁹⁸

(c) The Role of Parents: Finally, there’s no substitute for more parental involvement at all times. Parents need to accept the fact that this generation of children is growing up online and the kids are expressing themselves far more openly than did past generations.⁹⁹ This makes education and mentoring strategies essential.

Although it is true that many parents do not fully understand the modern, interactive technologies that their kids use and love, parents *do* know quite a bit about the importance of good behavior and proper etiquette. Perhaps the biggest problem in this debate is that parents are looking to government or Internet operators to solve problems that they’d rather not deal with. Talking to kids about online dangers or proper digital etiquette is not fun, but it is essential. And it should be done in an open, understanding, and loving fashion.

Dozens of excellent online safety websites offer parents excellent advice about how to begin this conversation with their children. Although not a comprehensive list, the following sites aggregate helpful tips, tools, and other information in one place:

- **GetNetWise.org** (www.getnetwise.org) is a public service website operated by the nonprofit Internet Education Foundation¹⁰⁰ and supported by a wide array of Internet and computer companies as well as a host of public interest

⁹³ www.nick.com/nicktropolis/game/index.jhtml?requestid=184748

⁹⁴ www.prweb.com/releases/2007/2/prweb501997.htm

⁹⁵ www.habbo.com/help/safetymonth/parentguide.html

⁹⁶ www.habbo.com/help/safetymonth/toolbox.html

⁹⁷ “MySpace Moves to Give Parents More Information,” *Wall Street Journal*, January 17, 2007, p. B1.

⁹⁸ “News Corp. Launches Online Safety Ages,” *CBS News.com*, July 13, 2006,

www.cbsnews.com/stories/2006/07/13/tech/main1799540.shtml

⁹⁹ Emily Nussbaum, “Say Everything,” *New York Magazine*, February 12, 2007,

<http://nymag.com/news/features/27341/>

¹⁰⁰ www.neted.org

organizations and child and family activists.¹⁰¹ GetNetWise website a comprehensive “Online Safety Guide” and lengthy inventory of “Tools for Families” that can be custom-tailored to the needs and values of individual families.¹⁰²

- **Internet Keep Safe Coalition** (www.iKeepSafe.org) is a coalition of 49 state governors and first spouses, law enforcement officials, the American Medical Association, the American Academy of Pediatrics, and many other corporations¹⁰³ and private associations (including many of the groups and sites listed below) that are dedicated to helping parents, educators, and caregivers by providing tools and guidelines to teach children the safe and healthy use of technology. iKeepSafe uses an animated mascot named “Faux Paw the Techno Cat” to teach children the importance of protecting personal information and avoiding inappropriate places on the Internet. The organization’s website offers a downloadable “10 Common Questions about Internet Safety” pamphlet¹⁰⁴ and several video tutorials to help parents set up various filters or controls.¹⁰⁵
- **Net Smartz Workshop** (www.NetSmartz.org) is produced by the National Center for Missing & Exploited Children and the Boys & Girls Clubs of America. This comprehensive website contains web safety tips and educational materials for parents, preteens, teens, educators, and law enforcement officials. They also sponsor a site devoted to younger children (www.netsmartzkids.org) that features interactive online safety games and videos.
- **Project Online Safety** (www.projectonlinesafety.com) is a collaborative online portal that offers a directory of online safety tools and educational materials developed by technology companies, media organizations and non-profits. Coalition members include: AT&T, BlogSafety.com, Cable in the Classroom, Charter, Comcast, Cox, Facebook, Fox Interactive Media (owner of MySpace.com), Internet Education Foundation, National Cable and Telecommunications Association, Network Solutions, Qwest, Time Warner Cable and the National Center for Missing and Exploited Children. Each organization provides an overview of its online safety efforts and links to various resources that parents can use to keep their kids safe online or to educate them about online dangers.
- **StaySafe.org** (www.staysafe.org) is an educational website sponsored by the Microsoft Corporation “intended to help consumers understand both the positive aspects of the Internet as well as how to manage a variety of safety and security

¹⁰¹ Major corporate supporters include Google, Microsoft, Verizon, Amazon.com, Yahoo, AOL, AT&T, Comcast, Dell, Earthlink, Visa, Wells Fargo, and the RIAA. Key public interest organizations include the Center for Democracy and Technology, the American Library Association, The Children’s Partnership, People for the American Way Foundation, National Consumers League, and many others.

¹⁰² See <http://kids.getnetwise.org/safetyguide> and <http://kids.getnetwise.org/tools>

¹⁰³ Corporate sponsors include AOL, Dell, Disney, Intel, Oracle, Siebel Systems, Symantec, and Yahoo! among others.

¹⁰⁴ www.ikeepsafe.org/iksc_partners/symantec/10_questions/Assets/TenCommonQuestions.pdf

¹⁰⁵ www.ikeepsafe.org/PRC/videotutorials/index.php

issues that exist online.”¹⁰⁶ The site contains specific sections for teenagers, parents, senior citizens, and educators with tips and tools tailored to each group.

- **i-SAFE Inc.** (www.iSafe.org) is a non-profit foundation whose mission is “to educate students on how to avoid dangerous, inappropriate, or unlawful online behavior. i-SAFE accomplishes this through dynamic K-12 curriculum and community outreach programs to parents, law enforcement, and community leaders. It is the only Internet safety foundation to combine these elements,” its website claims.¹⁰⁷ i-SAFE receives federal grants to support its efforts. The organization produces several monthly newsletters, including one for parents (“i-PARENT Times”) and one for educators (“i-EDUCATOR Times”), and it sells a wide variety of printed materials on online safety issues for classroom use.
- **WebWiseKids** (www.wiredwithwisdom.org) is a non-profit organization “committed to teaching children and their caregivers strategies for safe Internet use, including methods of detecting and deterring online predators.”¹⁰⁸ It specializes in interactive software and games that teach kids how to spot online threats and to deal with them promptly.
- **Wired Safety** (www.wiredsafety.org) bills itself as “the largest online safety, education and help group in the world. We are a cyber-neighborhood watch and operate worldwide in cyberspace through our more than 9,000 volunteers worldwide.”¹⁰⁹ The site offers educational services and online assistance and also reviews family-friendly websites, filtering software and other Internet services. Wired Safety also operators or works with several other affiliated online safety sites, such as:
 - **Wired Kids** (www.wiredkids.org) is geared toward youngsters and teens to help them understand online threats and to know how to deal with them.
 - **Teen Angels** (www.teenangels.org) “is a group of 13-18 year-old volunteers that have been specially trained by the local law enforcement, and many other leading safety experts in all aspects of online safety, privacy, and security. After training for six sessions, the Teenangels run unique programs in schools to spread the word about responsible and safe surfing to other teens and younger kids, parents, and teachers.”
 - **Net Bullies** (www.NetBullies.com) aims to protect kids from cyber-bullying.

Many other excellent websites that offer parents and kids outstanding advice for how to stay safe online, including: Net Family News,¹¹⁰ Family Tech Talk,¹¹¹

¹⁰⁶ www.staysafe.org/about.html

¹⁰⁷ www.isafe.org/channels/?ch=ai

¹⁰⁸ www.wiredwithwisdom.org/who_we_are.asp

¹⁰⁹ www.wiredsafety.org/information/about_us.html

¹¹⁰ <http://netfamilynews.org/index.shtml>

¹¹¹ www.familytechtalk.com

ProtectKids.com,¹¹² SafeKids.com,¹¹³ SafeTeens.com,¹¹⁴ BlogSafety.com,¹¹⁵ ChatDanger.com,¹¹⁶ Cyberbully.org,¹¹⁷ StopCyberbullying.org,¹¹⁸ and StopTextBully.com.¹¹⁹ Also, excellent examples of how other countries are dealing with the same issues can be found at BeWebAware.ca (Canada),¹²⁰ BeSafeOnline.org (Europe),¹²¹ and NetAlert.net (Australia).¹²²

Proper online etiquette is another subject that parents need to stress more with their children. Most parents repeatedly drill basic “offline” manners into their kids until it’s clear that they get it. Unfortunately, the same cannot be said for online manners. Again, this might be the case because the Internet and digital communications technologies have taken the world by storm and caught this current generation of parents a bit off guard. Unaccustomed to using modern computing devices or communications methods, some parents may be neglecting their duty to teach good online etiquette. Of course, as the National Academy of Sciences blue-ribbon panel noted, “It may be that as today’s children become parents themselves, their familiarity with rapid rates of technological change will reduce the knowledge gap between them and their children, and mitigate to some extent the consequences of the gap that remains.”¹²³

Regardless, here are a few lessons children need to be taught as they begin using interactive communications and computing technologies. To begin, kids need to learn to assume that *everything* they do in the digital, online world could be archived *forever* and will be available to future employers, romantic interests, their children and grandchildren, and so forth. This admonition needs to be repeated frequently to remind minors that their online actions today could have profound consequences for them tomorrow. Beyond this warning, children need to be encouraged to follow some other sensible rules while using the Internet and other interactive technologies:¹²⁴

- Treat others you meet online with the same respect that you would accord them in person;
- Do not cyber-bully or harass your peers;
- Do not post negative comments about your teachers or principals online;

¹¹² <http://protectkids.com>

¹¹³ www.safekids.com

¹¹⁴ www.safeteens.com

¹¹⁵ www.blogsafety.com

¹¹⁶ www.chatdanger.com

¹¹⁷ www.cyberbully.org

¹¹⁸ www.stopcyberbullying.org

¹¹⁹ www.stoptextbully.com

¹²⁰ www.bewebaware.ca

¹²¹ www.besafeonline.org

¹²² www.netalert.net.au

¹²³ Computer Science and Telecommunications Board, National Research Council *Youth, Pornography, and the Internet*, (Washington, D.C.: National Academy Press, 2002, p. 49.

¹²⁴ For a more extensive discussion of useful parental mentoring strategies, see Larry Magid and Anne Collier, *MySpace Unraveled*, pp. 131-149.

- Do not post or share inappropriate pictures of yourself or others;
- Avoid talking to strangers online;
- Avoid using lewd or obscene language online or in communications;
- Do not share your personal information with unknown parties;
- Talk to parents and educators about serious online concerns and report dangerous situations or harassing communications to them.

To better formalize such guidelines in the home, parents might want to ask their children to sign the “Family Netiquette Plan”¹²⁵ and the “Internet Respect Plan”¹²⁶ documents that the National Institute on Media and the Family produce. The one-page “contracts” contain many of the listed guidelines and ask both parents and children to sign the formal household agreement pledging to abide by those rules. Parents can then devise penalties if their children break the rules. The National Institute on Media and the Family recommends the following punishment if the rules are violated: “If there are any violations to expected behaviors, there will be no Internet, TV, or video games for the following three days except for necessary school work.”¹²⁷

It’s just another small part of a sensible carrot-and-stick approach to digital age parenting. “You need to take a holistic approach” to such problems, notes Ron Teixeira, executive director of the National Cyber Security Center.¹²⁸ Teixeira argues that it is essential that we drill basic lessons into our children—the digital equivalent of “don’t take candy from strangers,” for example—to ensure that they are prepared for whatever technologies or platforms follow social networking sites. “Education is the way you teach children to be proactive, and that will stay with them forever,” he rightly concludes.¹²⁹ As Parry Aftab of Wired Safety says, it’s about teaching our kids to “use the filter between their ears” and “make responsible decisions about their use of technology.”¹³⁰

Conclusion

Proposals to impose age verification mandates on social networking websites raise many sensitive questions with potentially profound implications for individual privacy and online freedom of speech and expression. That’s especially the case in light of the definitional ambiguities associated with “social networking.”

Protecting children from online dangers is a legitimate public policy concern, but age verification would not necessarily solve the problem it is meant to address. Perfect age verification is likely impossible, and history has shown that no technological control

¹²⁵ www.mediafamily.org/pdf_files/Network_Family_Netiquette_Plan.pdf

¹²⁶ www.mediafamily.org/pdf_files/Network_Internet_Respect_Plan.pdf

¹²⁷ *Ibid.*

¹²⁸ Quoted in Anick Jesdanun, “Age Verification at Social-Network Sites Could Prove Difficult,” *Associated Press Financial Wire*, July 14, 2006.

¹²⁹ *Ibid.*

¹³⁰ Parry Aftab, Filing in COPPA Rule Review 2005, June 27, 2005, p. 4.

is foolproof. Consequently, there is a very real danger that age verification regulations will create a false sense of security and encourage both children and parents to drop their guard. Worse yet, age verification mandates might create perverse incentives for children to evade online controls and might even encourage them to seek out offshore sites that are largely beyond the reach of domestic regulation or public pressure.

There are better ways to go about protecting our children within online environments. Parents and policy makers should embrace a “3-E” solution: Empowerment, Education and Enforcement. Empowerment refers to the tools and methods available to parents to better monitor and control their children’s online behavior and activities. Education refers to the need to industry, government and parents to do more to teach our children about online risks and proper online etiquette. And enforcement refers to the need for legislators and law enforcement officials to do more to weed out and adequately prosecute the real bad guys looking to prey on our children.

The Progress & Freedom Foundation is a market-oriented think tank that studies the digital revolution and its implications for public policy. Its mission is to educate policymakers, opinion leaders and the public about issues associated with technological change, based on a philosophy of limited government, free markets and civil liberties. The Foundation disseminates the results of its work through books, studies, seminars, conferences and electronic media of all forms. Established in 1993, it is a private, non-profit, non-partisan organization supported by tax-deductible donations from corporations, foundations and individuals. PFF does not engage in lobbying activities or take positions on legislation. The views expressed here are those of the authors, and do not necessarily represent the views of the Foundation, its Board of Directors, officers or staff.

The Progress & Freedom Foundation ■ 1444 Eye Street, NW ■ Suite 500 ■ Washington, DC 20005
voice: 202/289-8928 ■ fax: 202/289-6079 ■ e-mail: mail@pff.org ■ web: www.pff.org