THE HUFFINGTON POST
THE INTERNET NEWSPAPER: NEWS BLOGS VIDEO COMMUNITY

Larry Magid

Technology journalist

Parents Helping Young Kids Lie to Get Past Facebook's Age Restrictions

Posted: 11/ 1/11 01:24 PM ET

In May, Consumer Reports revealed that there were 7.5 million kids younger than 13 using Facebook, including more than five million 10 and under. In every case these kids had to lie to get around Facebook's rule that you must be 13 or older to join.

One might assume that these kids are also deceiving their parents, but that's often not the case. As I point out in my CNET blog, many parents are not only aware their kids are on Facebook but actually helped them set up the account.

Most parents know

A new study, "Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act,'" points out that:

- 95 percent of the parents whose 10-year-old was on Facebook knew about it
- 78 percent of them helped the kid sign up. Of all kids under 13
- 68 percent of parents helped their child create the account

- 78 percent of parents think it is OK for their child to violate minimum age restrictions on services

Overall, said the survey, "Almost three-quarters (74 percent) of parents whose child is on Facebook and who reported a minimum age knew that their child was on Facebook below what they believed the minimum age to be."

COPPA to Blame?

The primary reason that Facebook doesn't allow kids under 13 is because of the Children's Online Privacy Protection Act (COPPA). The law doesn't force companies like Facebook that collect personal information about users to block kids under 13, but it sets up a lot of road blocks including a requirement that the company get "verifiable parental consent." The process is expensive for companies and time-consuming for parents so, most companies that allow users to enter personal information, simply don't allow kids under 13.

COPPA was written back in 1998 -- long before Facebook -- to protect kids from revealing information to be used for marketing purposes and also to reduce their risk of exploitation. But, as the study's co-author danah boyd (her legal name is all lower case) pointed out in my CBS News / CNET interview (click to listen to MP3), "If you want to participate in social media, it's not that you can participate without giving over information, that simply is not possible." The whole purpose of Facebook is to share and you need to provide at least some personal information to use the service. The solution, said boyd, "is not to make it harder for them to lie."

In June, I blogged that Facebook ought to allow children under 13, because I think that it would be a lot safer to let them on in an age appropriate manner than to collectively bury our heads in the sand and pretend that they're not there. If this were the case, it should be accompanied by all sorts of parental controls as well as greatly increased privacy settings. I would also argue that the children to given an ad-free environment and that, of course, no information be used to market to them now or in the future. There should be a limit on who they can communicate with, but they should be allowed to use the service to interact with family members and others approved by their parents. As my ConnectSafely.org colleague Anne Collier pointed out in a NetFamilyNews post, there are plenty of good reasons why we should close the "communications gap," by allowing kids under 13 to communicate via popular social networking sites.

Facebook has indicated that it has no immediate plans to challenge COPPA and has no announced plans for finding a COPPA compliant way to welcome pre-teens. So, in the mean time, it will continue to block those who enter a date of birth that indicates they're below 13 and continue to remove the account of those who they catch after the account has been established.

The Federal Trade Commission is currently reviewing COPPA and is seeking comments from the public about proposed rule changes which, currently, do not include removing the under-13 restriction.

For more, see danah boyd's post Why Parents Help Tweens Violate Facebook's 13+ Rule and Anne Collier's Kids lying to Facebook, not their parents: Study.
*Disclosure: Larry Magid is co-director of ConnectSafely.org, a non-profit Internet safety organization that receives financial support from Facebook*and other Internet companies

Larry Magid

Technology journalist

Digital Citizenship & Media Literacy Beat Tracking Laws and Monitoring

Posted: 08/30/11 10:28 AM ET

(Credit: ConnectSafely.org)

As we start the school year, there are two trends in online child protection that are worthy of scrutiny. The first is the growing trend towards software and services that monitor what kids are doing online and with their phones. The second are proposed "do not track" laws that would require Internet companies to change the way they present advertising to children. Both have strong appeal but, like any strong medicine, there can be negative side effects. Another option -- the one that I prefer in most

cases -- is to teach digital citizenship and critical thinking, which, together, help children build skills and attitudes that will last a lifetime.

Do we really need to monitor our kids?

The trend towards monitoring is based on the assumption that kids will see and say dangerous or inappropriate things on the web and phones. Until recently the concerns were mostly about pornography and predators but now the focus is mostly on protecting kids from being bullied or becoming bullies as well as from posting content and images that could harm their reputation or get them in trouble. One example is "sexting," the sending of nude or sexually explicit images.

The products, which range from cloud based services that scour the Internet for any content by or about your child to computer software and phone apps that analyze content on the device, are mostly designed to look for clues that the child may be sending or receiving problematic messages or images or visiting inappropriate websites. The software or service notifies parents if something is suspicious, leaving it up to the parents to intervene as necessary.

The advantage is that a parent, armed with information on what his or her child might be up to, is in a position to provide guidance and turn a possible misstep into a "teachable moment." But one concern with this approach is whether the data being sent to parents could trigger a false alarm. Does the software fully understand the context of the words or actions it detects?

Also, kids can find work-arounds, by using devices or services that aren't protected by the software or by using phrases or spellings that the software isn't able to pick up. Some programs literally record everything the child does, which raises all sorts of issues including violation of the child's privacy and bombarding the parent with too much information.

The software between their ears

Regardless of whether you use parental monitoring tools, the most important child protection "software," is not the application running on the device or in the cloud, but the software running on that very adaptive computer between the child's ears. Monitoring or filtering services are never a substitute for helping children develop the critical thinking skills they need to protect themselves.

Just as surveillance cameras and police on the street won't protect adults from all misdeeds, monitoring and filtering programs won't protect kids from all potential problems online. Children need education and guidance to learn to make good decisions on their own, to protect themselves and treat others well.

Some of the leading monitoring programs include SafetyWeb, SocialShield, United Parents Child Protection Service, Trend Micro Online Guardian, Zone Alarm Social Guard and Norton Online Family. For more analysis and details on recent monitoring services and software, see this post by my ConnectSafely co-director, Anne Collier.

Do not track is a double-edged sword

I'm sympathetic to the motives behind legislation to "protect" children from advertising by passing "do not track" laws that limit information that companies can collect. While such legislation is well-intentioned, it may actually backfire.

The proposed laws would limit the ability of sites to place "cookies" and other tracking code on machines that trigger browsers to display targeted ads based on sites you've visited. For example, if a person visits websites dedicated to photography, they're more likely to see ads for cameras. While it might feel creepy to have such ads aimed at you, it's important to realize that these cookies are not reporting your name or other identifying information to companies but simply directing ads to your device. The result is that you are more likely to see ads about products that interest you than you are random ads aimed at the general population.

The major browsers have tools that enable you to notify web operators that you don't want to be tracked and most responsible ad networks have agreed to honor these requests. Users who opt out will still see ads, but they'll be more generic which means that they'll be less relevant. They also bring in less revenue to websites so prohibiting them could affect sites' ability to provide free content, drive them to charge for access or to put up more obtrusive and obnoxious ads.

Some argue that this opt-out approach is fine for adults but that kids should automatically be opted out of any tracking. But before we adopt technology designed to protect children, we need to make sure that it doesn't inadvertently jeopardize their privacy. My main concern about creating special advertising rules for minors is that it might require that the user be identified as a minor which would actually be a more serious invasion of their privacy than the status-quo.

Solution is critical thinking and digital citizenship

I realize that adults feel an obligation to protect children, but let's not under-estimate the ability for kids to actually make pretty reasonable decisions, especially if we embark on a campaign to create a truly digitally literate society, starting at a very young age.

What we need are educational campaigns that teach kids how to use whatever controls are built-in to the browsers, how to distinguish between advertising and editorial content and how to evaluate whatever information they come across to be able to make informed choices. The same skills that will protect kids from misleading advertising will also protect them from scammers, phishers, spammers, hackers and anyone else who would try to take advantage of them

Kids (and adults too) need to learn to critically evaluate what they see so that they become more resilient consumers or information.

Tools and laws sometimes have their place, but they're never a substitute for parenting, education, awareness and skills that help us and our children enjoy the benefits of the Internet safely and securely.

This post is adapted from an article that also appears on SafeKids.com and in the Palo Alto Daily News.

Follow Larry Magid on Twitter: www.twitter.com/larrymagid

THE HUFFINGTON POST
THE INTERNET NEWSPAPER: NEWS BLOGS VIDEO COMMUNITY

Larry Magid

Technology Journalist

Can YouTube for Schools Usher Education Into the 21st Century

Posted: 12/14/11 01:31 PM ET

for use in school. It's a great idea, but for it to actually be used in schools, many districts around the country will have to modify their filters to allow teachers to access at least this portion of YouTube.

Most schools have some type of filters in place designed to block pornography and other inappropriate material, and it's common for these filters to also block social media, including all of Facebook, MySpace and YouTube. Schools that accept federal E-rate funding are required to block materials that are obscene, depict child pornography or are harmful to minors -- but there is nothing in the federal rules that require schools to block social media.

Treat social media like books and sports

It's a good thing schools don't treat books and sports the way most treat social media.

There have always been books that are inappropriate for a school setting. But rather than ban all books, schools allow the ones that support their curricula and encourage children to explore literature in general. When it comes to sports, schools recognize that there are dangers -- every year, lots of children are injured and some die from sports related injuries. But rather than ban sports, schools embrace them and make sure that kids have good coaches, safety equipment and rules to ensure fair play.

Of course we could just let the kids play in the street without any training, Of course we could just let the kids play in the street without any training, supervision or mandatory safety equipment. That's how many schools approach social media -- including such things as videos on YouTube or resources on social networking sites.

It's not as if kids are staying away from social media just because they can't use it at school. They're using it at home, at friends' houses and -- via their mobile devices -- anywhere they happen to be. It's not as if kids are staying away from social media just because they can't use it at school. They're using it at home, at friends' houses and -- via their mobile devices -- anywhere they happen to be. Their non-school hours are filled with use of technology and social media. Maybe schools ought to put a sign at the front gate that reads, "You are now leaving the 21st century."

Teachers and parents as social media partners

It's time for teachers -- and parents -- to become young people's partners in the use of social media. Just as we teach reading and supplement the use of books with great mentors in the classroom and encourage fair play and skill development with coaches on the athletic field, we need to incorporate educators into our kids' use of social media.

I'm not suggesting that kids be allowed to polish off their Facebook profiles in school or dish the dirt with their online friends while they should be paying attention in class. But completely blocking domains like Facebook.com or YouTube.com denies kids access to some incredibly useful material.

There are thousands of Facebook pages dedicated to a wide variety of subjects that can be used in schools. If you search for "Facebook education," you'll find links to numerous ways that Facebook and other social media can help teachers supplement their existing materials. One article that comes up in that search, "100 Ways You Should be Using Facebook in Your Classroom" lists some incredibly useful projects like encouraging kids to follow news feeds relevant to course material, share book reviews, practice a foreign language, create their own news source, keep up with politicians, post class notes, brainstorm and lots more.

Even more than Facebook, Google's YouTube can be an incredibly useful resource in school. Sure, there are plenty of inappropriate videos on the user-supplied service. But there is also a wealth of resources from a very wide variety of sources, including the Smithsonian Institution, the Massachusetts Institute of Technology, UC Berkeley, PBS, TEDTalks and the amazing educational videos from Kahn Academy, which are used in schools throughout the world. You can find some of this material -- along with tips on how to use YouTube in the classroom -- atYouTube.com/teachers. Because many schools simply ban YouTube, these incredible resources are not available for use in the classroom. Kids can watch them at home or on the way to school via the mobile devices, but not on school computers. Preventing distractions such as videos of cats dancing on a piano or keeping kids from age-inappropriate videos in school makes sense, but not at the expense of preventing kids and teachers from accessing a vast library of educationally sound videos.

As part of the launch of "YouTube for Schools" (schools can sign up at youtube.com/schools), Google is encouraging school districts to open up their filters so that teachers can accessYouTube.com/edu. Hopefully school administrators will see the value in this and find ways to unblock at least this portion of YouTube.

Disclosure: Larry Magid is co-director of ConnectSafely.org, a nonprofit Internet safety organization that receives financial support from Facebook and Google.

This article also appeared in the San Jose Mercury News and on SafeKids.com.

Follow Larry Magid on Twitter: www.twitter.com/larrymagid

THE HUFFINGTON POST
THE INTERNET NEWSPAPER: NEWS BLOGS VIDEO COMMUNITY

Larry Magid

Technology journalist

Rise in Social Media Correlates with Safer Experiences for Teens

Here's a shocker for some. By two important measures, teens are safer online now than they were before the advent of social media.

A new report from the Crimes Against Children Research Center (CCRC) found a decline in 2010 of both unwanted sexual solicitations and unwanted exposure to pornography compared to studies conducted in 2005 and 2000.

According to a 2011 report from the Pew Internet & American Life Project, "95% of all teens ages 12-17 are now online and 80% of those online teens are users of social media sites."

As I wrote in my CNET News blog, a 2010 survey of 1,500 youth between 12 and 17 found that 9 percent had received an unwanted sexual solicitation in the past year. This compares to 13 percent in 2005 and 19 percent in 2000. In all three studies, some of those unwanted sexual solicitations came from other youth, and the vast majority of them were not "aggressive." Only 3 percent of the youth in 2010 said that offline contact was attempted or made. Most youth did not find the solicitations to be frightening or disturbing. That's actually a bit lower than the 4 percent who had aggressive solicitations in 2005 and identical to the 2000 figure.

There was a small rise in the percentage of youth who experienced some type of online harassment during the 12 months preceding the survey. Eleven percent had experienced harassment in 2010, compared with 9 percent in 2005 and 6 percent in 2000.

Although sometimes used to indicate cyberbullying, harassment is not the same as bullying. The survey asked youth, "Did you ever feel worried or threatened because someone was bothering or harassing you online?" Bullying (cyber and otherwise) is defined by the Olweus Bullying Prevention program and most other experts as "aggressive behavior that involves unwanted, negative actions," along with "a pattern of behavior repeated over time" that "involves an imbalance of power or strength."

The mostly good news comes at a time when the majority of American youth are using social media, most notably Facebook. The first survey took place years before Facebook or MySpace, and the 2005 study before most teens were using Facebook (Facebook wasn't open to high school students until September 2005). Correlation doesn't necessarily imply causation, so I'm not suggesting that Facebook has necessarily caused unwanted solicitation or pornography to decline, but it obviously hasn't caused it to increase.

Could Social Networking Be Diverting Kids from More Dangerous Sites?
I'm speculating, but I do wonder, though, whether a case could be made that social media has made kids safer and less prone to unwanted pornography. For one thing, kids are now spending time in sites like Facebook instead of chat rooms, which were always the most problematic venue for unwanted solicitation. Moreover, Facebook and most other social networking sites prohibit nudity and other sexually explicit content, so while kids are on Facebook, they are very unlikely to stumble into pornography. Again, I don't have data to support this, but it sure seems likely.

The authors of the study made the same observation, pointing out that "youth have migrated from chat rooms to social networking sites over past several years. In social networking environments, youth may be confining more of their interactions to people they know, thus reducing online unwanted sexual comments or requests."

Disclosure: *Larry Magid is co-director of ConnectSafely.org, a nonprofit Internet safety organization that receives financial support from Facebook, Google, Tagged, and other social media companies.*
This post also appears on SafeKids.com.