ConnectSafely
Smart Socializing Starts Here™


September 24, 2012

TO: The Federal Trade Commission
FR: Anne Collier and Larry Magid
Co-Directors of ConnectSafely.org
Former Co-Chair and Education Committee Chair, the Online Safety & Technology Working Group (OSTWG)
RE: Comment on 2012 revisions to COPPA

As long-time youth advocates and active participants in consumer education for youth online safety and privacy for 15+ years, we have followed developments with the Children's Online Privacy Protection Act since its early development. While there is no question that the intention to update COPPA is good, the potential outcomes of increasingly detailed updates are greatly concerning, due to the nature of today's Internet.

As the title of the Online Safety & Technology Working Group (OSTWG) 2010 report to Congress, "Youth Safety on a Living Internet," was meant to indicate, the increasingly social, user-driven nature of the Internet and digital technologies – most especially where young people's use of them are concerned – makes it very difficult to regulate that use without unintended negative consequences in terms of children's safety and privacy, children's opportunities, and innovation in technology, media, and business. As OSTWG's co-chair (Anne) and education committee chair (Larry), we spent a great deal of time helping to craft a document to provide Congress with effective strategies to ensure safety and privacy while encouraging digital literacy and citizenship education for children in both home and school settings nationwide. The OSTWG found that, in a user-driven media environment that serves as a platform for nearly every form of expression and behavior in real time, education is by far the most effective protection.

Unintended consequences for children

We worry that some of the proposed revisions could put children at greater risk. The proposal to define an IP address as personally identifiable information is one example. While, in some cases, it is theoretically possible to identify the device or household associated with an IP address, that data is not readily available to site operators who have access to IP addresses of visitors. In most cases it would take a court order to reveal that information. Requiring verifiable parental consent would also require that parents identify the actual child behind the IP address, presenting a much bigger risk to the child's privacy than the address itself.

In the case of embedded content, the risk of requiring consent is even greater. For example, if a YouTube video embedded in a family or child-friendly site requires verifiable consent to both the operator and Google, the effect is to require parents to disclose personally identifiable information to both parities.

In addition to disclosing more information to more parties than necessary, the process could put an additional burden on already beleaguered parents and encourage young users to go to less compliant sites that have less age-appropriate content and don't require parental consent.

In addition, increasing the number of occasions where parents are required to give consent increases the likelihood of kids developing workarounds (for example the commonly known one of children lying about their age) or avoiding compliant services altogether. The most compliant services become the least attractive by being the most burdensome to both children and parents. This is the central problem of youth safety in an international medium where there are always "places" where children can go which do not comply with U.S. law.

Even the most basic requirement of COPPA – not gathering personal information without verifiable parental consent – can put some children at greater risk. For example, if a child under 13 is showing clear signs of depression and talking about harming himself in communication with other children in a COPPA-compliant virtual world that, under its compliance, does not gather personal information about the child, the service is unable to provide any contact information to 911 or others who can provide emergency care to that child. Another example is, if a child is threatening physical harm to another child in an online game, the COPPA-compliant game host has no personally identifiable information that could be used to reach caregivers or law enforcement in the offending child's offline life to help resolve the situation. These are actual consequences of COPPA to date.

Burden on small business and thus on children

In the interest of protecting children's privacy, the COPPA rule obviously increases companies' cost of doing business. One of the consequences of that reality is that large companies are better able to absorb the costs than start-up companies. This restricts small site operators and app developers and limits innovation and opportunities for new products that could benefit young Internet users.

A consequence for child safety in this increased cost of doing business for small companies is a decreasing ability to afford the most effective child-protection measure they can provide: human moderators, or community managers. Better than any technology, human moderators detect patterns of behavior, analyze problems, troubleshoot, and create solutions. If the presence of human moderators is priced out of children's online services, the children's part of the Web and mobile platform will become less safe, having the opposite effect for which COPPA was intended.

In the interplay of large and small businesses

Obviously we're seeing the emergence of "ecosystems" of providers and third parties on the Web and mobile platforms. An updated COPPA rule should make it practical for platform operators such as Apple, Google and Facebook to enable parents to provide verifiable consent to the platform which can then pass it on to app developers – most of whom are very small businesses with few if any resources for collecting consent on their own – with the understanding that the developers must adhere to COPPA guidelines or be subject to being kicked off the platform as well as to any potential civil or criminal consequences. We believe that the COPPA rule would benefit from further exploration – *with* the parties involved, both providers and third parties – of best practices and functions for platform systems (both Web and mobile). In the ever-evolving nature of technology, the last thing we want is for people to look back at COPPA revisions a few years from now and say, "that's so 2012."

The on-the-ground reality in homes and for businesses is the increased burden that increased protections place on users, a burden that is all too easy for young users to avoid by moving on to less compliant services, which in turn…

1. Reduces protection for children and
2. Lowers revenue for business, which…
3. Chills innovation and business opportunities in children's digital media and thus…
3. Restricts children's options for safe, creative spaces in digital media.

To summarize, there is a careful balance to strike between providing effective protections that don't send children "underground" while keeping COPPA up-to-date with constantly changing technology, and we are concerned that the proposed revisions are weighted too much on the latter side of the scale. In keeping with the spirit of COPPA, we want to see regulations that establish a general framework of protecting children from flagrant privacy violations without suppressing children's own speech and opportunities. And while we agree that industry needs guidelines and a set of ethical boundaries, we worry about creating regulations that could have the unintended consequences of greater risk to children's safety and privacy and could quickly be outdated as technology evolves.

Sincerely,

Anne Collier and Larry Magid
Co-Directors
ConnectSafely.org