# Deconstructing Reaction to Net Safety Task Force Report

January 16, 2009

Now that the dust is settling on the release of the Final Report [1] of the Internet Safety Technical Task Force, I want to highlight a few important points that have been raised this week. The Task Force was formed through an agreement between MySpace and 49 state Attorneys General to look at technology that might be used to protect kids in social networking environments. The AGs were clearly looking for a technological "silver bullet" to address what they and the popular media have portrayed as huge risks for kids on social networks; they didn't get it.

The Task Force - run by the Berkman Center at Harvard Law School - reached a set of conclusions that undercut the common myths underlying the AGs assumptions. In simple terms, the Task Force concluded that: -- the risks to kids online are much less, and different, than popular perception holds, and -- there are no technologies that can or should be mandated or imposed to "solve" the risks that kids do face online (like teen-on-teen cyberbullying). No one denies that being online carries some risk for kids (and adults, too). But a strong conclusion of the Task Force is that education is a critical way to address the risk, and that there are not technological silver bullets that governments should mandate.

Here are a few additional points about the final report, the reactions to it and beyond, that are worth highlighting:

**Some AGs claim the report used** old, out-dated data to show only a minimal risk to kids in social networking environments. That assertion is simply not true, as a full reading of the lengthy Research Advisory Board report [2]will show. The Task Force relied on the best data available, **and** the best researchers. The Research Advisory Board had **all** of the leading academic researchers who study online risk to kids involved in developing the research report, and their conclusions are that risks online are much more subtle and of a different nature than the popular media suggests.

**The AGs should "show me the data"** if they continue to believe that there is a massive risk to minors in social networking contexts; they must come forward with concrete, testable data to make their case. Right now, all the AGs can offer are anecdotal assertions that kids can get in trouble online. The Task Force certainly agrees that some kids do in fact get in trouble online, but the report shows that those same kids are probably in trouble offline, too. Anecdotally, it appears that most online predator cases involve chat rooms, **not** social networks, and equally critically, most of those cases involve sting operations where a predator connects with a law enforcement official posing as a minor looking for sex online. The anecdotal evidence, taken together, does not suggest that the average minor using one of the leading social networks is in fact at any greater risk online than offline.

**The media overlooked a key point in the study**, namely that the Task Force looked closely at 40 different technologies that were submitted to it, and concluded that none of the technologies were appropriate to be required for use by social networks. The Task Force created a Technical Advisory Board to review the 40 submissions, and I served as an "Observer" on the TAB and was the only Task Force member to closely review and submit written comments [3] on each of the technologies proposed. So I can report from first hand review that although some of the technologies are useful in some contexts, none is appropriate for legislatures to mandate.

The TAB reviewed some excellent "user empowerment" technologies that allow parents and caregivers to monitor, guide and even limit kids' use of social networking sites. Other submissions offer forensic technologies that might be very useful for law enforcement. But many of the technologies proposed some form of "age verification," which the TAB correctly concluded was not a workable, effective solution for social networking sites that are intended for a global audience that includes **both** minors and adults. AV technology may well be useful to create, for example, a

U.S.-focused adults-only site, or for use in financial transactions like online liquor sales. But for the leading social networking sites - which are global in reach and which welcome both adults and minors - AV technology would not help. Moreover, AV technologies cannot easily verify the ages of minors, and most of the technologies would create privacy and other problems that would outweigh any benefits they might have. Finally, many of the technologies would create serious First Amendment and constitutional problems if they were to be required by law to be used.

**Task Force member Aristotle's attack** on MySpace for supposed "destruction" of information about Registered Sex Offender activities is grossly inappropriate and off base. First, this is a prime example of "no good deed goes unpunished" - MySpace voluntarily decided to remove known RSOs from its site, and then it ends up being a primary target of attack based on these RSOs. Second, until a law enforcement official determines that one or more of the RSOs removed from MySpace in fact was engaging in criminal or threatening conduct, it would be inappropriate for MySpace to disclose information about those individuals in the absence of a subpoena. Third, were MySpace to do what Aristotle advocates, then MySpace would violate its own privacy policy, and thereby subject itself to significant risk of legal liability for that breach. At bottom, MySpace has made it very clear that it cooperates with the AGs and law enforcement subpoenas relating to these RSOs. If Aristotle thinks that not enough is happening about these RSOs, then it should be urging law enforcement to open more investigations of possible criminal conduct. But to suggest, as Aristotle does, that MySpace should turn itself it the prosecutor, judge, and jury about these RSOs is in my view inappropriate. That should be up to law enforcement, not a private company.

**Everyone should just step back, take a breath** and realize that there is risk in life, and neither parents nor governments can eliminate all risk for kids. Whether we as parents like it or not, social networks are now part of the American social fabric for young people. Our focus should be on educating kids about the risks online, not - as some legislators have suggested - trying to prevent kids from going online or using social networks. I noted a recent study [4] that the Centers for Disease Control & Prevention discussed that shows that every year there are more than 50,000 serious snowboarding accidents in the U.S., and a majority of the victims are young people. But I think most people would think it absurd for state legislatures or AGs to advocate that ski resorts should deny service to minors, or use age verification technology to figure out who is a minor. Snowboarding - just like social networking - is an activity that parents let their kids do **even though** there is some modest level of risk. A core conclusion of the Task Force is that the risk online is not in fact significantly different or greater than the risk offline. We should all work together to minimize risk both online and offline, but our society does not (and should not) try to eliminate **all** risk to kids (or we should start with prohibiting minors from being in cars, because as the CDC says, "Motor vehicle injuries are the greatest public health problem facing children today"). Tens of millions of American kids have hundreds of millions of online interactions every day, and the vast majority of those interactions are safe and healthy. We absolutely need to address and reduce risk online, but we should not destroy social networking to eliminate all risk.

**Unintended Consequences** A final note is that we must be careful of unintended consequences. A New York Times editorial [5] in late December described how laws across the country regulating where Registered Sex Offenders can live - and prohibiting RSOs from living near schools and daycare centers - have had the unintended consequences of **reducing** the ability of the state to monitor RSOs (because many RSOs have been forced into a homeless life), and **reducing** the ability of RSOs to live a structured, non-criminal lifestyle. The Times editorial summed up the situation:

The problem with residency restrictions is that they fulfill an emotional need but not a rational one. It's in everyone's interest for registered sex offenders to lead stable lives, near the watchful eyes of family and law enforcement and regular psychiatric treatment. Exile by zoning threatens to create just the opposite phenomenon - a subpopulation of unhinged nomads off their meds with no fixed address and no one keeping tabs on them. This may satisfy many a town's thirst for retributive justice, but as a sensible law enforcement policy designed to make children safer, it smacks of thoughtlessness and failure.

I fear that our society is about to make a similar mistake with social networks. If we impose laws that inhibit minors from using social networks, we will drive them away from the current leading social networks (which are very concerned about child safety) to overseas websites (which have far less

concern about the safety of our kids). If there is one takeaway that policymakers should get from the Task Force report, it is that public policy in this area should be made based on real data about real risk, not media hype, and on a concrete understanding of the technological, privacy, free speech, and other implications of any proposed policy (or technology) solution. The news media has well covered the report, including the New York Times [6], Wall Street Journal [7], and Computerworld [8]. And a number of other Task Force members have posted thoughtful blog posts on the report, including Adam Thierer [9], Anne Collier [10], and Larry Magid [11].

- 
- Social Networking
- ISTTF
- Age Verification



**Links:**
[1] http://cyber.law.harvard.edu/pubrelease/isttf/
[2] http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report-APPENDIX_C_Lit_Review_121808.pdf
[3] http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ObserverComments_CDT.pdf
[4] http://www.cdc.gov/ncipc/E-News/2008/06-12-2008.doc
[5] http://www.nytimes.com/2006/12/30/opinion/30sat1.html
[6] http://www.nytimes.com/2009/01/14/technology/internet/14cyberweb.html?_r=1
[7] http://online.wsj.com/article/SB123187498732078111.html
[8] http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9126040&source=rss_topic13
[9] http://blog.pff.org/archives/2009/01/internet_safety_9.html
[10] http://www.netfamilynews.org/2009/01/major-crossroads-isttf-report-released.html
[11] http://news.cnet.com/8301-19518_3-10142096-238.html?tag=newsLatestHeadlinesArea.0