

The Privacy Paradox of Adolescent Online Safety: A Matter of Risk Prevention or Risk Resilience?

Pamela Wisniewski | University of Central Florida



Networked technology is an ever-present force in the lives of nearly all teens; according to Pew Research, 92 percent of teens (ages 13 to 17) in the US go online daily, 73 percent have access to smartphones, and 71 percent engage in more than one social media platform.¹ Some argue that the prevalent use of mobile smartphones and social media has created a “tethered” society, which facilitates a wide array of new social interactions but also amplifies online risks. The Crimes against Children Research Center reports that 23 percent of youth have experienced unwanted exposure to Internet pornography, 11 percent have been victims of

online harassment, and 9 percent report receiving unwanted sexual solicitations online.²

While concerning, these exposure rates do not indicate that online risks are an epidemic, nor do they necessitate moral panic; in fact, there is little evidence that online risk presents more harm than the risks teens typically encounter offline. Yet, the fear that teens will certainly fall victim to unthinkable online dangers persists, shaping the technologies designed to keep teens safe online. This article challenges the current solutions for protecting teens online and suggests a paradigm shift toward empowering teens to be agents of their own

online safety by teaching them how to self-regulate their online experiences.

A Paradox between Safety and Control

The “privacy paradox” traditionally points to the discrepancy between individuals’ stated privacy concerns versus their conflicting disclosure behaviors, such as oversharing on social media. However, when Barnes first coined the term over a decade ago,³ she specifically referred to the online dangers (that is, sexual predation) posed to teens due to their over-willingness (that is, lack of concern) to share personal information via social media combined with their paradoxical desire to protect their publicly posted private thoughts from their parents.

The assumption that teens are at risk online because of their poor disclosure decisions is prevalent in the literature, resulting in a body of research focused on increasing teens’ concern for privacy as a way to reduce their online disclosures, thereby protecting them from encountering online risks. Ironically, this “privacy as prevention” approach to online safety has resulted in privacy-invasive tools that now allow parents to monitor and restrict their teens’ online behaviors,⁴ which only exacerbates the privacy tensions between parents and teens.⁵

On one hand, we are telling teens that they need to care about

their online privacy to stay safe, and on the other, we are taking their privacy away for the sake of their online safety. This catch-22 poses a “new” privacy paradox for our youth that needs to be addressed when designing future technologies to protect teens from online risks. In her book, *It’s Complicated: The Social Lives of Networked Teens*, boyd argues, “as a society, we often spend so much time worrying about young people that we fail to account for how our paternalism and protectionism hinders teens’ ability to become informed, thoughtful, and engaged adults.”⁶

My past work illustrates why paternalistic and abstinence-oriented approaches to adolescent online safety simply fall short. In traditional families, communication regarding the risks teens experience online is particularly poor; parents tend to be overly judgmental and overreact when teens disclose their online risk experiences, making the problem worse.⁵ Overall, restrictive parenting practices have a suppressive effect, reducing risks but also opportunities for moral growth and beneficial online engagement. Parent-focused approaches to adolescent online safety also assume a significant level of privilege; teens, especially those who are most vulnerable to online risks (for instance, foster youth), often do not have parents who are actively engaged in ensuring their online safety. Finally, such approaches do not teach teens how to effectively protect themselves online.⁷

Teens, Privacy, and Online Safety

The assumption that teens lack the ability to make calculated privacy decisions online has been debunked; teens do take protective measures against online risks and value their privacy, but they also value the social benefits of engaging online.^{6,7} As such, teens exhibit a markedly different privacy

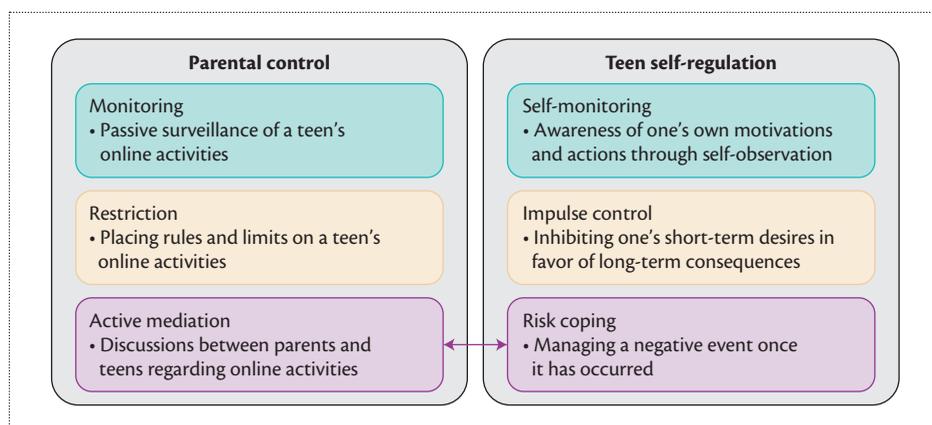


Figure 1. Conceptual framework of Teen Online Safety Strategies (TOSS).

calculus than adults; they treat “risk as a learning process,” taking protective measures to recover once disclosures have escalated to the point of potentially harmful interactions.⁷ Some level of risk taking and autonomy seeking is a natural and necessary part of adolescence, and preventing such experiences may actually stunt developmental growth as teens strive to individuate themselves from their parents. Thus, new interventions for adolescent online safety need to reflect how teens manage their online privacy, not how we do as adults. Therefore, the long-term goal of design-based interventions for adolescent online safety should be to teach youth how to effectively manage online risks as they transition into adulthood, not just to shield them from online risks.

Moving toward Risk-Resilient Teens

Adolescent resilience theory is a strength-based approach developed to explain divergent outcomes related to various teen risk behaviors, including substance abuse, violent behavior, and sexual promiscuity.⁸ Resilience is an individual’s ability to thrive in spite of significant adversity or negative risk experiences. Our research has confirmed that resilience plays a significant role in protecting teens

from the negative effects of Internet addiction and online risk exposure.⁹ Teens are often able to cope and resolve negative online experiences without intervention from their parents, even benefiting from experiencing some level of online risk by learning from their mistakes and developing crucial interpersonal skills, including boundary setting, conflict resolution, and empathy.⁷ Therefore, we developed a new conceptual framework of Teen Online Safety Strategies (TOSS), which attempts to shift the balance and rectify the privacy paradox between parents and teens. It was theoretically derived to illustrate the tensions between parental control and teen self-regulation when it comes to teens’ online behaviors, their desire for privacy, and their online safety (Figure 1).

In the TOSS framework, parental control strategies for online safety include:

- *Monitoring*: passive surveillance of a teen’s online activities,
- *Restriction*: placing rules and limits on a teen’s online activities, and
- *Active mediation*: discussions between parents and teens regarding their online activities.

Teen self-regulation strategies were drawn from the adolescent

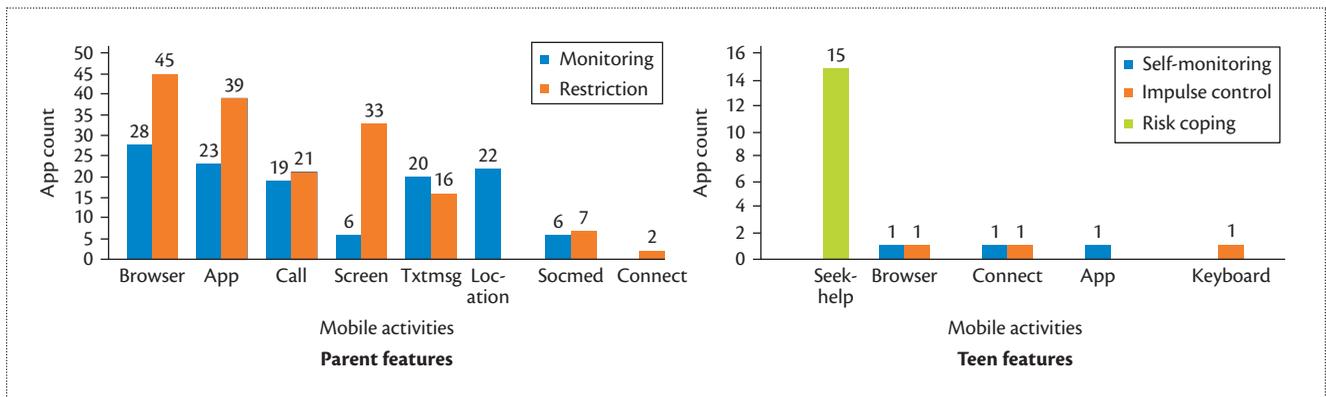


Figure 2. Parent versus teen features within mobile online safety apps.

developmental psychology literature, which considers self-regulation a “resiliency factor” that protects teens from offline risks by modulating emotions and behaviors through monitoring, inhibition, and self-evaluation. Teen self-regulation strategies include *self-monitoring*, *impulse control*, and *risk coping*.

For teens to effectively self-regulate their online behaviors, they must be aware of their own actions through self-observation (that is, self-monitoring). Impulse control aids in self-regulation by inhibiting one’s short-term desires in favor of positive long-term consequences. Risk coping is a component of self-regulation that occurs after one encounters a stressful situation, which involves addressing a problem in a way that mitigates harm. Because risk coping is influenced by teens’ own appraisals of online risk as well as that of their parents’, the TOSS framework makes an explicit association between active parental mediation and teen risk coping.

A Critical Assessment of Where We Are Now

In two recent studies, we applied the TOSS framework to better understand the commercially available technical offerings that support adolescent online safety, and what teens thought about these

applications. First, we analyzed the features within 75 commercially available mobile apps on Android Play that had the primary or secondary purpose of promoting teen mobile online safety.⁴ By downloading and exploring the apps, we identified 42 unique features (for instance, monitoring and restricting web browsing, app installations, calls, screen time, and so on) with 382 instances of these features being supported across the apps in our dataset.

An overwhelming majority of features (89 percent) within these apps supported parental control through monitoring (44 percent) and restriction (43 percent), as opposed to facilitating parents’ active mediation or supporting any form of teen self-regulation. Many of the apps were extremely privacy invasive, providing parents granular access to monitor and restrict teens’ intimate online interactions with others, including browsing history, the apps installed on their phones, and the text messages teens sent and received. Teen risk coping was minimally supported by an “SOS feature” that teens could use to get help from an adult (Figure 2).

Based on these results, we argue that existing apps do not reflect positive family values (for instance,

trust, respect, and empowerment) that meet the needs of teens or parents. Essentially, we are telling teens that they cannot be trusted and that we, as adults, must protect them from any dangers they may encounter in online spaces. Such fear-based messages do little to empower teens and, arguably, to keep them safe online.

In a follow-up study, we analyzed 736 reviews of these parental control apps that were publicly posted by teens and younger children on Google Play.¹⁰ We found that the majority (79 percent) of children overwhelmingly disliked the apps, while a small minority (21 percent) of reviews saw benefits to the apps. Children rated the apps significantly lower than parents; the mean difference between parents’ mean score was 1.87 (95 percent CI [confidence interval], 1.76 to 1.98) higher than children’s mean score, $t(793.34) = 33.77, p < 0.05$.

We conducted a thematic content analysis, which uncovered that teens, and even younger children, strongly disliked these apps because they felt that they were overly restrictive and invasive of their personal privacy, and negatively impacted their relationships with their parents. Many reviews suggested that the apps were so restrictive that the children could not

longer accomplish everyday tasks, such as doing their homework:

“It doesn’t just protect you from the porn and stuff, it protects you from the whole internet!! It wouldn’t let me look up puppies!...If I can give it less than a star I would!!”
—One Star, Net Nanny for Android, 2014

They also thought that the online safety apps completely violated their personal privacy and equated the apps to a form of parental stalking:

“Fantastic. Now now my mom is stalking me. I have nothing to hide. You can always just ask to go through my phone. Too invasive and down right disrespectful. Thanks for the trust, mom.”
—One Star, MamaBear Family Safety, 2014

These children were very vocal in their opinions about the apps not aligning with good parenting techniques, such as communicating with them or trusting them to make good decisions:

“Seriously, if you love your kids at all, why don’t you try communicating with them instead of buying spyware. What’s wrong with you all? And you say we’re the generation with communication problems.”
—One Star, SecureTeen Parental Control, 2016

Comparing our results through the TOSS framework (Figure 3), the reasons why teens and younger children disliked these apps aligned directly with the TOSS dimensions for parental control—which were the online safety strategies that our earlier study found were well-supported by these apps. We found that reviews were more positive when children felt that the apps afforded them more agency (that

	Feature analysis N=75 apps	Teen reviews (N = 736 reviews)
Parental control (89% of app features)	Monitoring (44% of app features)	Apps were too privacy invasive (23% of negative reviews)
	Restriction (43%)	Apps were overly restrictive (35%)
	Active mediation (<1%)	Apps supported bad parenting/ lack of communication (14%)
Teen self-regulation (11% of app features)	Self-monitoring (2% of app features)	Apps gave more freedom and ability to negotiate with parents (12% of positive reviews)
	Impulse control (<1%)	Apps helped them control unhealthy behaviors (23%)
	Risk coping (4%)	Apps helped keep them safe (17%)

Figure 3. Summary of research findings.

is, self-regulation) or improved their relationship with their parents (that is, active mediation). For instance, some children found apps useful when they helped them control unhealthy or addictive behaviors (that is, impulse control) or gave them more awareness of their unhealthy behaviors (that is, self-monitoring). They were open to using online safety apps when they saw direct benefits, such as managing unhealthy behaviors.

A takeaway from this research is that, as researchers and designers, we should consider listening to what teens have to say about the technologies designed to keep them safe online and conceptualize new solutions that engage parents and respect the challenges teens face growing up in a networked world.

A Possible Path Forward

During adolescence, teens need personal and psychological space for positive development; privacy also becomes very important in terms of the parent–teen relationship to build trust and allow teens a level of personal autonomy. To compromise on solutions that may meet both parents’ desire to keep their children safe and teens’ desire to

uphold personal privacy, we make a number of design recommendations targeted toward app designers to increase teen adoption and acceptance of mobile safety apps by thinking of teens as their end users.

Empower Teens as End Users

Encourage teens to use mobile apps to self-regulate their own behaviors (as opposed to being forced to use an app by their parents). Few teens are going to opt to install an app that explicitly says that it is for “parental control,” which was the most common moniker in commercially available apps. Prompting teens to use mobile online safety apps themselves and engaging with teens directly as end users may empower teens by giving them more agency and choice, thereby increasing their sense of personal autonomy and control.

Use a Teen-Centric Approach to Design

Provide features teens find personally beneficial. We should leverage user-centered techniques to better understand what mobile safety features teens would actually find useful. Instead of assuming that teens are inherently risk seeking, a

more nuanced approach would be to ask them in what ways they feel that they need to be kept safe. For instance, we found that some teens liked apps that helped them disconnect from their phones or reduce other problematic behaviors. Therefore, teens may prefer “personal assistant”-type features that assist (not restrict) them in being more aware of their unhealthy behaviors and changing them without parental intervention. These features could keep track of teens’ activities via their smart devices and “nudge” them whenever an inappropriate behavior is detected.

Design for Safety with Privacy in Mind

Create online safety apps that employ a level of abstraction to give parents helpful meta-level information regarding teens’ mobile activities instead of full disclosure of what teens do from their mobile phones. For example, an app may provide parents a high-level summary of who their teen is engaging with via their mobile device and how often, as opposed to divulging the content of every conversation.

Help Teens Communicate with Their Parents

Provide features so that teens can negotiate with parents. In cases when teens’ perceptions of appropriate online behaviors conflict with their parents’, it would be helpful for online safety apps to provide flexible parental controls that support and are more contingent on appropriate contexts of use, giving teens the ability to negotiate with their parents in particular circumstances. For instance, more app designs may consider implementing features similar to the “reward time system” offered by the Screen Time Companion app that allows teens to get extra time if they meet certain criteria specified by their parents. Reward systems are more

contextualized restraints because they provide positive reinforcement and allow teens to earn privileges, as well as their parents’ trust.

By taking a more “teen-centric” instead of a “parent-centric” approach to adolescent online safety, researchers and designers can help teens foster a stronger sense of personal agency for self-regulating their own online behaviors and managing online risks. Technology should support teens in their developmental goals, including information seeking, learning about rules and boundaries, and maintaining social relationships, in addition to keeping them safe from online risks. However, this goal will only be accomplished once we listen more intently to teens as end users. As such, we call for new design practices that are more teen-centric and place value on online safety as an integral part of their adolescent and developmental growth, teaching teens the skills and giving them to confidence to engage safely and smartly with others through the Internet. ■

References

1. A. Lenhart, *Teens, Social Media & Technology Overview 2015*, Pew Research Center: Internet, Science & Tech, 2015.
2. L.M. Jones et al., “Trends in Youth Internet Victimization: Findings from Three Youth Internet Safety Surveys 2000–2010,” *Journal of Adolescent Health*, vol. 50, no. 2, 2012, pp. 179–186; <https://doi.org/10.1016/j.jadohealth.2011.09.015>.
3. S.B. Barnes, “A Privacy Paradox: Social Networking in the United States,” *First Monday*, vol. 11, no. 9, 2006; <https://doi.org/10.5210/fm.v11i9.1394>.
4. P. Wisniewski et al., “Parental Control vs. Teen Self-Regulation: Is There a Middle Ground for Mobile Online Safety?,” *Proceedings of the 2017 ACM Conference on Computer*

Supported Cooperative Work and Social Computing, 2017, pp. 51–69.

5. P. Wisniewski et al., “Parents Just Don’t Understand: Why Teens Don’t Talk to Parents about Their Online Risk Experiences,” *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 2017, pp. 523–540.
6. d. boyd, *It’s Complicated: The Social Lives of Networked Teens*, Yale University Press, 2014.
7. P. Wisniewski et al., “Dear Diary: Teens Reflect on Their Weekly Online Risk Experiences,” *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 2016, pp. 3919–3930.
8. F. Stevenson and M.A. Zimmerman, “Adolescent Resilience: A Framework for Understanding Healthy Development in the Face of Risk,” *Annual Review of Public Health*, vol. 26, 2005, pp. 399–419.
9. P. Wisniewski et al., “Resilience Mitigates the Negative Effects of Adolescent Internet Addiction and Online Risk Exposure,” *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015, pp. 4029–4038.
10. A.K. Ghosh et al., “Safety vs. Surveillance: What Children Have to Say about Mobile Apps for Parental Control,” to be published in *Proceedings of the 2018 ACM Conference on Human Factors in Computing Systems*, 2018.

Pamela Wisniewski is an assistant professor at the University of Central Florida. Contact at pamwis@ucf.edu.



Read your subscriptions through the myCS publications portal at <http://mycs.computer.org>