It's Still Complicated

From Privacy-Invasive Parental Control to Teen-Centric Solutions for Digital Resilience

Jinkyung Katie Park, Mamtaj Akter, and Pamela Wisniewski | Vanderbilt University
Karla Badillo-Urquiola | University of Notre Dame

We discuss the paradigm shift from restrictive approaches toward resilience-based solutions to promote adolescents' online safety and well-being. We describe how restrictive strategies induce a tradeoff between teens' privacy and online safety and present empirical studies that examine resilience-based approaches.

According to a Pew Research report on teens, social media, and technology, 96% of U.S. teens use the Internet daily; 46% of them are online almost constantly. Most teens have access to digital devices, such as smartphones (95%), desktop or laptop computers (90%), and gaming consoles (83%).[1] A significant majority of teens reported that being social online helps them feel connected, creative, and supported. Nonetheless, recent research has associated prolonged screen time, cyberbullying, exposure to mature media content, and problematic Internet usage with mental health issues and physical safety concerns, such as online sexual grooming and sex trafficking.

As a result, the news media and scholarly research have disproportionately emphasized the necessity for restrictive measures aimed at curtailing access to technology to safeguard teens. The heightened attention from fear-based media narratives has bolstered legislative efforts by U.S. Senators Blumenthal and Blackburn in proposing the Kids Online Safety Act (KOSA),[2] aimed at shielding children from online risks. While this legislation has positive aspects, some advocacy groups, such as those that support the rights of LGBTQ+ youth and freedom of speech, have expressed concerns regarding the heavy use of digital surveillance impeding the privacy, safety, and access-to-information rights of adolescents.

Adolescence represents a distinct developmental phase bridging childhood and adulthood, with a primary objective of growing toward independence and autonomy. Adolescents are often described as "digital natives" who grow up with digital technologies and are natively tech savvy. However, digital natives might actually be better termed *digital naives* because most teens are still forming the critical knowledge of how personal information flows and how to look for accessible information in a networked environment.[3]

In today's digitized world, one of the most important developmental tasks for adolescents is to acquire proficiency in managing online interactions and safeguarding themselves against digital risks. Meanwhile, society has made assumptions that adolescents are at extreme risk because of naive digital literacy and lack of privacy awareness and that online risk is an epidemic that plagues adolescents. As a result, paternalistic and restrictive strategies (e.g., parental control apps) have been implemented as a means to protect adolescents from online risk. The existing literature indicates that teens perceive such restrictive strategies as privacy invasive.[4] In addition, such restrictive approaches may hinder opportunities for adolescents' healthy development.

Digital Object Identifier 10.1109/MSEC.2024.3417804

Copublished by the IEEE Computer and Reliability Societies

In 2014, in the book *It's Complicated: The Social Lives of Networked Teens*, Boyd cautioned scholars and society at large against restrictive strategies for adolescent online safety:

> 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. Regardless of the stories in the media, most young people often find ways to push through the restrictions and develop a sense of who they are and how they want to engage in the world.[3]

Over the past decade, scholars have explored how restriction falls short in mitigating adolescent online risk and shifted the narratives to empowering teens through digital resilience. In this article, we provide a brief overview of this paradigm shift that moves away from privacy-invasive and restrictive strategies toward teen-centric solutions for adolescent digital privacy and resilience. Specifically, this article highlights the following:

- a critical shift from restrictive parental control measures to resilience-based, teen-centric approaches, acknowledging the evolving digital autonomy of adolescents and emphasizing the importance of empowering them to manage online risks effectively
- an overview of research that focuses on the effectiveness and implications of teen-centric and resilience-based approaches, which offers evidence-based insights for parents, practitioners, and policymakers
- key design implications for parents, designers, practitioners, policymakers, and researchers in the space of privacy and adolescent online safety for building privacy-protective and resilience-promoting online safety solutions.

In doing so, we discuss recent legislative efforts and their potential impacts on adolescent privacy and autonomy, hence contributing to the critical analysis of how legal frameworks intersect with adolescent online safety and rights. In addition, we introduce a socioecological perspective to adolescent online safety, thereby contributing to a more nuanced understanding of the multifaceted nature of online safety and the diverse factors influencing adolescents' digital experiences. As such, we shed light on the transition from privacy-invasive parental mediation methodologies toward teen-centric strategies inclusive of vulnerable, marginalized, or at-risk adolescents aimed at enhancing their online privacy and safety.

Related Work

Adolescence is a unique developmental stage in which the primary developmental objective is to successfully grow toward independence and autonomy. Developmentally, adolescents are characterized as those between the ages of 10 and 19. In the digital privacy literature in the U.S. context, however, the age range for adolescents is often described as between the ages of 13 and 17, focusing on the legal implications of being a minor in the United States. (The U.S. Children's Online Privacy Protection Act legally protects children under the age of 13 from unfair or deceptive collection, use, and/or disclosure of their personal information by online service providers, while age 18 is the legal definition for adulthood.)

During adolescence, teens need autonomy to individuate themselves from their parents. As they become more social than younger children, they appreciate online engagement. Some level of risk-taking and autonomy-seeking is a natural and necessary part of adolescence, and preventing such experiences may impede their developmental growth to individuate themselves from their parents. From a developmental perspective, adolescents are aware of online privacy risks; hence, they make careful decisions about information disclosure and balance their desire to protect themselves with the desire to socialize online.[5] Although there is little evidence that online technology creates more harm than benefits for teens, mounting concerns around how social media and the increased use of personal digital devices negatively impact adolescent development and mental health have led to a moral panic. This has led to restrictive approaches that aim to shield adolescents from online experiences rather than teaching and empowering them to be resilient against these new online challenges.

This trend toward paternalistic approaches to protect youth online is evidenced by state-level legislation to ban TikTok and social media use for younger teens; civil mass tort lawsuits against social media platforms; and national legislation, such as the KOSA in the United States, a comprehensive bipartisan legislation proposed by U.S. senators in 2022.[2] This proposed legislation mandates that commercial platforms, including but not limited to social media platforms, take proactive measures to mitigate harm to minors, such as addressing issues related to the promotion of self-harm, suicide, and sexual exploitation. Furthermore, it necessitates independent audits and encourages public scrutiny from experts and academic researchers to ensure that these platforms are effectively undertaking meaningful actions to address risks faced by teens.

All of these may have good intentions but, to some extent, may ignore or dismiss adolescents' agency as

well as their rights to information, freedom of expression, digital technology, and civic engagement. For instance, teen privacy advocates are concerned that the enactment of KOSA may incentivize social media platforms to gather even more data about children to prevent a specific set of harms to minors. Unintentionally, KOSA could lead social media platforms to use broad content filtering measures, limiting minors' access to certain online content, such as sex education tailored for LGBTQ youth, which schools had previously implemented in response to earlier legislation. As such, while restrictive approaches to adolescent online safety may offer protection from online risks, they may also come at the expense of the digital privacy rights of teens and opportunities for teens to access valuable online resources and support, particularly salient for vulnerable teens who do not have support systems. Therefore, taking a fear-based and controlling approach disproportionately focused on adolescent vulnerability does not prepare teens for future online adversity, nor does it productively advance the field. What is needed, then, involves new insights from empirical study and a multidimensional interpretation of the context surrounding adolescent behaviors and experiences online.

Over the past decade, Dr. Pamela Wisniewski and colleagues have examined evidence-based and teen-centered approaches that empower adolescents by enhancing risk-coping, resilience, and self-regulatory behaviors so that they can learn to protect themselves more effectively from online risks. In this article, we summarize the concepts and outcomes from collaborative work that shift the narratives from restriction toward evidence-based and teen-centered online safety solutions for digital resilience. As such, this article provides implications for parents, designers, practitioners, policymakers, and researchers in the space of privacy and adolescent online safety.

Restriction as a Means to Protect Adolescents From Online Risk

The landscape of adolescent online safety is complex, with evolving strategies to mitigate risks and foster responsible digital behavior. Parental mediation, ranging from monitoring to active engagement, significantly influences adolescents' online experiences. While restrictive mediation approaches monitor and regulate online activities, active mediation strategies prompt discussions on balancing protection with autonomy as teens mature. Concurrently, sociotechnical interventions, like age verification and risk detection, aim to enhance safety by restricting access to inappropriate content and identifying threats in real time. However, concerns about privacy, surveillance, and adolescent autonomy emphasize the need for nuanced approaches to empowering teens to manage their online risks. This section explores parental control, sociotechnical interventions, and regulatory measures in adolescent online safety, revealing the challenges and overlapping interests involved.

Parental Mediation for Adolescent Online Safety

Parental mediation encompasses a spectrum of strategies, ranging from restrictive mediation and monitoring to active mediation. Restrictive mediation, such as parental control apps, involves parents limiting their children's access to social media or establishing rules regarding appropriate media content and exposure. Parental control applications are frequently employed to monitor teens' online activities, providing parents direct access to teens' online content, such as visited websites, geolocation data, text messages, call logs, and mobile app usage (e.g., the Life360 location-sharing app and the Bark parental control app). Such approaches are particularly pertinent for younger children and adolescents (aged eight 12), aiming to shield them from premature exposure to adult media content. However, teens mostly find parental control tools invasive and damaging to their relationship with their parents. Therefore, instead of restricting and stalking their children, parents will have to use active measures to educate children about the security and privacy threats online.[4]

As adolescents mature, they require opportunities to develop skills in risk assessment, problem-solving, and seeking help to independently manage potential online risks. Additionally, relying solely on restrictive approaches to online safety may be ineffective in protecting adolescents from online risks, as it limits the potential opportunities for youth to interact with others online. Therefore, active digital parenting practices, such as open communication about online risks, the joint use of digital technologies with teens, and the facilitation of access to beneficial online content, are important, as they foster youth development toward safe and autonomous online engagement. Such active mediation is effective, as it involves parents having discussions with their children regarding the undesirable aspects of media consumption and advising them on appropriate ways to engage with media content.

However, parent- and family-centric approaches to adolescent online safety often assume a significant level of privilege, as they require considerable parental time and attention, and they may be even influenced by other aspects of the parent–child relationship dynamic. Moreover, communication about online risks with

teens is often challenging, as parents may react judgmentally or excessively when teens disclose their online experiences, exacerbating rather than mitigating the issue. Consequently, it can erode trust between parents and teens as well as undermine positive family dynamics. What is worse is that the teens most vulnerable to online risks, such as those in foster care, often lack parental support to actively ensure their online safety. Hence, scholars advocate for sociotechnical solutions that shift away from relying solely on parental mediation toward empowering adolescents to self-manage their online risks to be resilient.[5]

Age Verification and Online Risk Detection

In recent years, several sociotechnical interventions aimed at bolstering adolescent online safety have been examined, including age verification and automated online risk detection. Age assurance entails technical measures designed to ascertain the age or age range of users, employing various methods with differing degrees of certainty (e.g., through ID checks or face recognition-based age estimation) and within the context of varying levels of online risk. A range of age assurance measures is commonly utilized to limit teens' access to goods, services, and digital content, although such measures are susceptible to circumvention or offer limited protection to teens in high-risk environments. As highlighted in the euConsent report, teens can readily bypass these measures, for instance, by utilizing their parents' IDs. Third-party age verification methods (e.g., digital IDs) tend to be more effective, although they may engender safety or privacy concerns, such as online fraud. Furthermore, parents seek the autonomy to make informed decisions regarding the content and services their teens access based on their decisions of what is appropriate for their teens rather than on general age restrictions.[6]

Another trend is the use of artificial intelligence-based tools to detect a wide variety of harmful online content, largely within big technology companies. Given the magnitude of the online content under scrutiny, the adoption of automated detection mechanisms is gaining momentum, as the human-based alternative is deemed largely unfeasible. The underlying premise of data-driven risk detection technology posits that the systematic collection of personal data enables the identification of emerging threats, facilitating targeted and proactive interventions. However, the compilation of datasets to train machine learning (ML) algorithms introduces additional privacy and surveillance concerns, as it necessitates the utilization of data pertaining to adolescents' intimate and risky behavioral interactions (e.g., instances of sexual grooming), which often transpire through private channels.

Privacy-Preserving and Resilience-Based Approaches to Adolescent Online Safety

The majority of teens perceive the aforementioned restrictive measures as excessively intrusive and constraining.[7] In response to these perceived conflicts, adolescent online safety researchers have called for teen-centered approaches where teens have some level of privacy and autonomy in making their own online safety decisions. The key idea around this approach is the shift from an authoritarian view of protecting teens to more supportive frameworks that can empower teens to self-regulate and manage online risks meaningfully.[5,7] This underscores the necessity for the adoption of strength-based design practices that can empower teens and parents to manage online risks in meaningful ways. In this section, we summarize research that moves beyond traditional approaches, which rely on restrictive and privacy-invasive mechanisms, toward resiliency and autonomy-based design that can empower teens to utilize their knowledge to self-regulate and cope in the face of online risks.

Intentional and Meaningful Media Use

Amid the proliferation of engagement features, such as autoplay and recommendation algorithms, across social media platforms, researchers are actively investigating strategies to alleviate adolescents' challenges with addictive media consumption and time management. This arises from the notable gap between adolescents' heightened sensitivity to social stimuli and their self-regulation skills. Developmentally, skills pertaining to self-regulation, including reflection, strategic planning, goal-setting, and self-assessment, are relatively underdeveloped during adolescence. Consequently, there has been an effort to design interventions aimed at facilitating adolescents' intentional and planned use of digital media.

For instance, Davis et al.[8] designed and developed a mobile application called *Locus* that prompts adolescents to reflect on their social media usage throughout the day and establish goals for the following day. Locus is a wrapper application that allows users to open social media apps directly through the Locus app. After opening the Locus app, users can view the list of all social media apps installed on their devices. When users select a specific social media app, they are shown a text-based reflective prompt before being taken to the desired app asking, "What would make you feel good about your time on Twitter today?" Responding to this entry prompt is optional and be done via text or speech input. Locus also sends a general notification once per day at 9 p.m. asking, "How do you think you'll use social media tomorrow?" Through a two-week experimental study involving pre- and postsurveys and exit interviews with

adolescents aged 14–18, Davis et al. found that adolescents exhibited enhanced self-control and autonomy in managing their social media consumption, coupled with reduced instances of unintentional usage. Teens shared that they felt a heightened sense of purpose and empowerment in their interactions on social media platforms.

As such, intentional and planned media usage has long been recognized as an effective means of fostering self-regulation, particularly from early childhood. With initial guidance from parents, adolescents are capable of acquiring intentionality and making goal-oriented decisions as part of planned usage, which serves as a catalyst for self-regulatory development. By allowing adolescents to establish their own healthy boundaries, intentional and preplanned media use can alleviate privacy tensions between parents and teens, especially those who struggle with negotiating conflicting boundaries. At the same time, Davis et al. observed considerable individual variation among adolescents in the "just right" level of support for their self-regulation behaviors on social media.[8] This indicates the need for designing interventions considering factors such as gender, age, socioeconomic status, and race as well as the role of individual characteristics and motivation to change one's social media use. In addition, adolescents' engagement with social media could be varied for social media platforms with different affordances. Therefore, how to tailor interventions to cater to adolescents with different needs and expectations as well as differing social media environments is a crucial design consideration that warrants further investigation.

Youth-Centered Risk Detection

From a human-centered perspective, collecting ground-truth annotations from those who experience the risk ensures that the training risk detection models reflect real-world experiences and accurately represent the risks users face online. Risk perceptions are highly subjective; therefore, understanding the risk perceptions of people who experienced the risk (i.e., adolescents in our case) is the foundation of the design of ML-based sociotechnical systems to support them. In an effort to build teen-centric ML systems, researchers explored ways to work with teens to collect ecologically valid online risk data. For instance, Razi et al.[9] built an online system to collect youth-donated Instagram data. Researchers created a secure website where youth participants could fill out a survey about their social media usage and unsafe experiences, upload their Instagram data, and annotate their own data (e.g., conversation) as "safe" or "unsafe." If unsafe, they annotated for risk type and risk level, the context for each conversation around why it made them feel unsafe, and the relationships between conversation partners.

The dataset resulted in building automated systems to identify risky media, sexual conversation, and suicide ideation with high accuracy. It also allowed researchers to provide valuable insights into understanding the context and multidimensionality of online risk teens experience in private settings, as these are pivotal for designing youth-centric and customized risk prevention strategies to promote youth resilience from online risk. For instance, using the youth-provided labels for the level of risk (i.e., high risk versus low risk), researchers were able to build ML algorithms to prioritize identifying high-risk cases for prompt risk mitigation, while the algorithms take more time to take into account the conversation context for a more accurate understanding of the risk context for low-risk cases. The idea of building customized algorithms for differing levels of online risk is that there are cases where rapid responses are critical to prevent imminent risk (e.g., suicide), while there are other cases where an accurate understanding of conversation context is needed to avoid false alarms (e.g., content moderation). As such, by taking human-in-the-loop approaches (i.e., working with youth to share their risk data and annotate for risk experience themselves) to design automated risk detection algorithms, researchers have been able to move toward youth-centered and context-aware "real-time" risk detection models as "just-in-time" interventions to mitigate their online risk experience.

In the meantime, building risk detection with data donation approaches could face challenges, ranging from the technical issues of dealing with gathering a sensitive dataset to ethical considerations. One major technical challenge, as noted by Razi et al., was the compatibility between Instagram's data and the data collection systems. Instagram frequently changes how it organizes and formats user data, necessitating continuous technical updates to the system. More importantly, collecting online risk data from minors requires increased precautions, considering the complexity and sensitive nature of private data. Therefore, a series of additional measures beyond the institutional review (e.g., National Institutes of Health Certificate of Confidentiality, risk mitigation documents, and mandated reporting protocols) are needed to ensure the privacy, confidentiality, and safety of participants.

Co-designing Online Safety Solutions

Co-design methodologies have been applied in adolescent online safety research to integrate the unique perspectives of teens in the development of teen-centric online safety solutions. One notable initiative is the establishment of a youth advisory board (YAB) program, which represents a long-term co-design

endeavor aimed at involving teens in the design of their own online safety and privacy solutions. Over the course of a year, researchers engaged with a cohort of seven teens, aged 15 to 17, with the objectives of 1) imparting user experience (UX) design skills and familiarity with industry-standard tools, along with offering career development guidance; 2) soliciting direct feedback on research protocols related to adolescent online safety and involving them in research studies; and 3) involving them in co-design activities tailored to their interests.[10]

As part of the YAB, researchers explored methodological approaches, such as the asynchronous research community (ARC) environment in which asynchronous weekly discussions were facilitated on Discord, along with synchronous design sessions conducted on Zoom. Asynchronous activities were conducted through text responses and screenshots, while design activities were conducted using Figma, where teens created their own design solutions for new online safety features. In synchronous meetings, researchers worked in longer sessions with teens to co-design and conceptualize their online safety ideas. Asynchronous follow-up discussions were done on Discord, where all members could give feedback and suggestions on their continuing design work.

Over the eight-week period of ARC activities, researchers identified that teens perceived different social media platforms as a spectrum of privacy levels, such as private platforms, public platforms, and semipublic platforms. Teens exhibited a conscious decision-making process in selecting social media platforms based on their goals and preferences, demonstrating awareness of potential privacy risks. For instance, teens preferred more private platforms for one-to-one interaction but switched to more public platforms when viewing or sharing content. This suggests that teens are well aware of the privacy risks they may encounter on social media platforms. Consequently, to achieve a balance between meeting their objectives and mitigating privacy concerns, teens employed diverse strategies to regulate their privacy settings according to the intended audience.

Accordingly, their design ideas for privacy features centered on aiding them with more granular control over determining what information on their accounts could be shared with whom. These insights, collectively, underscore the inadequacy of one-size-fits-all solutions in fostering online safety for teens with distinct aspirations and objectives. Instead, a nuanced understanding of teens' individual motivations and perspectives on social media usage as well as their privacy perceptions is crucial for tailoring customized support systems to facilitate safer online experiences.

However, engaging in remote settings made it difficult for teens to establish rapport and trusted connections with researchers and other teens. For instance, teens from the work by Ali et al.[10] shared that there was a lack of peer-to-peer interactions, which hindered their participation and the development of long-term connections. In addition, they faced this issue in the ARC environment (i.e., Discord), as teens took part in the activities at their own discretion, and their timings varied inconsistently. This led to irregular and fragmented interactions with other teens and researchers, inhibiting good peer-to-peer relationships to work together effectively.

Therefore, building rapport with teens and accommodating teen participants with diverse needs and skill sets could be keys to tackling challenges associated with co-design approaches. Balancing between synchronous and asynchronous modes is also important to promote flexibility and encourage individual contributions from quieter teens. Invest time and effort to share common ground and interests. Office hours, co-design, and in-person meetings (if possible) can help better rapport and team building, with more opportunities to build trusting relationships. Finally, provide opportunities for group activities and interactions to help teens develop peer-to-peer connections, build networks, and increase motivation for participation.

Evaluating Nudge-Based Intervention

Real-time or "just-in-time" nudge-based interventions are also proposed to support teens at the moment when they experience risks online. *Nudges*, defined as subtle cues intended to influence behavior, are being investigated as effective means of guiding adolescents' actions without removing their autonomy. For instance, Agha et al.[11] co-designed online safety nudges with teens as part of their UX Bootcamp study, where teens created storyboards regarding their past online risk experiences. Their risk experiences guided the creation of the public cyberbullying nudge that filtered a risky comment and highlighted community guidelines while giving options to view, delete, or report the risk. The private information breaching nudge warned users of requests for location-revealing sensitive information, allowing them to continue, ignore, or block. The private predatory risk nudge warned about inappropriate messages from a stranger, with options to continue, leave, or block the sender. The private scam and explicit content nudge used filters to censor the risk, with choices to view, delete, and inform others.

With these real-time nudges designed with teens, Agha et al. moved forward with co-designing social media situation platforms to evaluate online safety nudges with teens. The rationale behind

employing simulated environments lies in the endeavor to assess the impact of nudges on promoting safe online decision-making among adolescents, all within settings that closely mirror real-life scenarios while safeguarding teens from real risks. Therefore, Agha et al. risk scenarios and nudge designs to a cohort of 20 teens to refine the designs. Teens were asked to redesign at least one or more of the risk scenarios and nudges with high-level feedback to make them more realistic and effective. Feedback was provided through design annotations on FigJam, along with verbal discussions.

They found that teens co-designed risk scenarios that were subtle and higher in risk to be believable, perpetuated by risky personas that tricked the teen by establishing trust or a shared context. Teens recommended nudges for risk prevention through personalized sensitivity filters, with the autonomy to view the risk. Moreover, teens expressed a desire for proactive coping mechanisms, measures to hold perpetrators accountable, and educational community guidelines. In terms of evaluating these nudges, the majority of participants expressed a preference for simulated social media environments wherein they could observe tangible behavioral changes without exposure to actual risks. Concurrently, teens emphasized the importance of transparency regarding the collection and recording of data to address any privacy concerns stemming from their involvement in the study.

Meanwhile, we recognize that the implementation of real-time online safety nudges is not simple, as they rely on the accurate detection of risk at the right moment. Although the just-in-time behavioral interventions discussed can be effective in adolescents' decisions toward their online safety, they cannot cater to all adolescents with different digital experiences and needs. For the interventions to be effective, they need to be context aware, which, in many cases, relies on techniques such as ML-based risk detection. Therefore, collaborative efforts bridging the design space and technical implementation of the designed systems are crucial to moving toward providing personalized nudge-based intervention.

Moreover, as nudges influence one's behaviors, the most prominent ethical concern related to nudging is that it could compromise adolescent autonomy. In the context of adolescent online safety, risk prevention requires content moderation and censorship, which are considered a breach of freedom of speech in many contexts. However, teen participants in the study by Aga et al. perceived that controlled and personalized ways of filtering unsafe content respected their decision-making autonomy. In addition, teens believed that moderating harmful content was necessary and that compromising an individual's freedom of speech was reasonable if it protected minors from online harm.[11] Therefore, nudges that prompt the perpetrator to reconsider their actions, along with the freedom to continue—but not without consequences—should be carefully designed.

Socioecological Approaches to Adolescent Online Safety

The landscape of adolescent online safety has shifted toward collaborative family-based approaches, fostering communication, privacy, and autonomy within digital family contexts. Recent studies have investigated joint family oversight mechanisms, enabling parents and teens to make decisions together and providing teens the autonomy to support themselves and their families in online risk management. These innovations signal a move toward collaborative models, recognizing the varied needs within families. However, while family-centric strategies remain prevalent in industry and policy discourse, there is a growing recognition of the limitations of solely relying on parental mediation, particularly for vulnerable youth without robust familial support systems. This section lays the groundwork for examining the socioecological framework, which integrates digital parenting with broader social systems to promote resilience and community-based support in adolescent online safety.

Family-Based Collaborative Approaches

In recent years, researchers have explored the implementation of collaborative family-centric approaches to address adolescent online safety concerns. These approaches aim to facilitate open discussions within families while respecting teens' privacy and autonomy in making not only their own online safety decisions but also decisions related to their families' mobile privacy and security. Taking a joint approach focused on teens' online safety, Akter et al.[12] designed and developed a joint family oversight application, Community Oversight for Privacy and Security (CO-oPS), that allowed parents and teens to have an equal footing in monitoring one another's mobile app usage and permission settings as well as providing feedback. The CO-oPS app allowed family members to review each other's installed apps and the privacy permissions granted or denied, facilitating direct knowledge exchange between parents and teens and enhancing communication. They also had the ability to hide some of their installed apps from one another, ensuring equal levels of personal privacy for both parents and teens.

Through a lab-based user study with 19 parent–teen dyads, Akter et al. explored the applicability of this approach in helping teens and their parents collaboratively manage their mobile online safety, security, and privacy. They found that, while teens were the primary

providers of technical support within the household, parents often resorted to manual inspections of their teens' phones or employed parental control apps to restrict the installation of new applications. When evaluating the CO-oPS app, both parents and teens saw value in the ability to review each other's apps and permissions, as it enhanced transparency regarding app usage within the family and facilitated discussions surrounding apps and permissions. When they reviewed one another's apps and permissions, parents showed more concerns regarding their teens' app usage, perceiving it as a potential gateway for outside individuals to connect with their teens online. Conversely, teens primarily focused on identifying risky permissions granted on their parents' devices, demonstrating a heightened awareness of the malicious intentions of third-party mobile applications.

Overall, Akter et al. highlighted how parents and teens conceptualized mobile privacy, security, and online safety differently and how joint family oversight can potentially benefit in enhancing both parents' and teens' learning of mobile privacy, security, and online safety through fostering comonitoring and communication. However, these advantages would rely heavily on both parent and teen buy-in to recognize their mutual responsibility for each other's online well-being, necessitating a paradigm shift from prevailing approaches to adolescent online safety, such as parental control, to more collaborative joint family approaches.

In sum, collaborative joint family approaches showed potential in adolescent online safety. These approaches promoted transparency, privacy, and autonomy and facilitated discussions on mobile privacy and security within families. Through these approaches, parents and teens exhibited differing perceptions of mobile online safety, privacy, and security, highlighting the need for collaborative family-based solutions in adolescent online safety to enhance joint learning in families.

Beyond Family-Based Approaches

Parent- and family-focused technology mediation approaches (e.g., parental control applications) continue to be the most widely recommended strategies by industry and policymakers. However, this perspective on online safety overlooks the reality that the most vulnerable youth to online risks, e.g., youth in foster care, often do not have engaged parents or family members who can actively employ these strategies. Furthermore, research by Badillo-Urquiola et al.[13] with foster parents and caseworkers demonstrates that even those responsible for the well-being of these youth receive little to no support and struggle with keeping them safe online. Caseworkers are often overworked, with limited availability to address online safety concerns, while foster parents are overly stressed, with so many responsibilities that they are desperate for solutions.

Therefore, recent efforts in adolescent online safety advocate for approaches that leverage the socioecological support systems of youth, that is, the different people and factors that influence a youth's online experience. These individuals and factors can be defined at different levels, such as the individual level, relationship level (family and peers), and community level (school). For instance, Badillo-Urquiola et al. observed tensions between caseworkers and foster parents that could be alleviated by working together to manage the online safety challenges of foster youth. They recommended developing collaborative sociotechnical systems that could bring caseworkers and foster parents into partnership with one another. In this sense, a sociotechnical system can act as an interpersonal-level system that connects caseworkers, foster parents, and foster youth to increase support.[13] In our proposed conceptual model (see Figure 1), the social ecologies of the adolescent resilience framework are combined with digital parenting practices across the adolescent life span to promote the shift between restrictive parental mediation in early childhood to self-regulation supported by social ecologies in adolescence. This framework helps change the online safety narrative from one focused on parental control to one that considers the range of mediation strategies that promote social connections and leverage community-based supports.

Beyond "One-Size-Fits-All" Approaches

While privacy-preserving and resilience-based online safety solutions show positive trends toward promoting the digital well-being of teens, we must acknowledge how different factors (e.g., socioeconomic status, cultural background, and digital access) affect adolescents' online experiences and risks and how teen-centric solutions can be adaptable to diverse needs and contexts. For instance, teens in foster care are even more susceptible to higher levels of online risk, such as sex trafficking. However, foster parents often lack the technology expertise to effectively manage teens' user of technology. As a result, they resorted to restrictive practices.[13] Online safety technologies in which the power is balanced between the stakeholders of the foster youth's support system and the foster youth are needed to empower them to make their own decisions and learn. However, few evidence-based interventions to empower foster youth self-regulation and online safety have been developed. Therefore, the new systems should be developed for and with foster youth with input from foster parents and caseworkers.

Moreover, much of the discourse around online safety currently emerges from the Global North (e.g.,

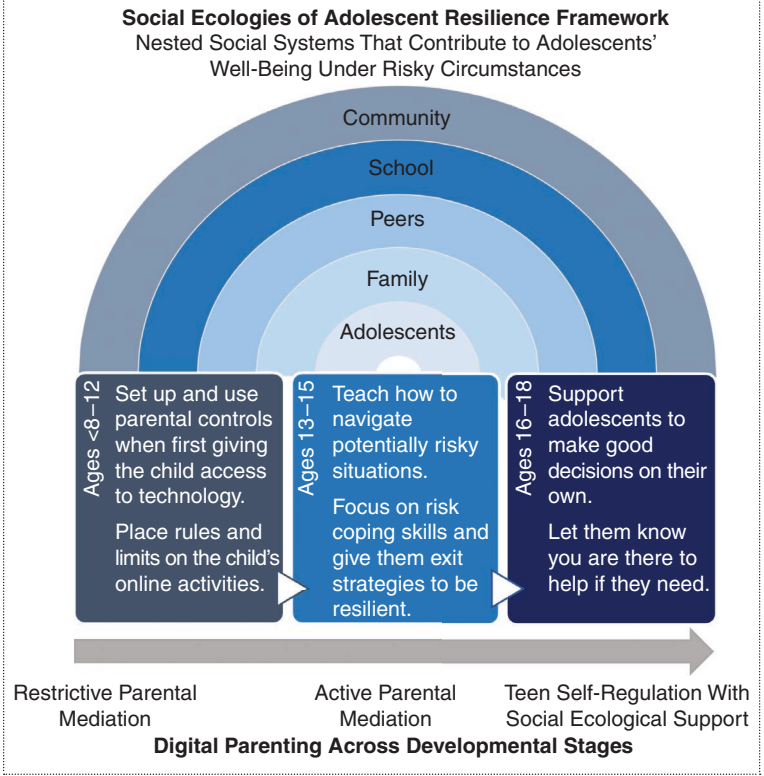

Figure 1. A social–ecological approach to digital parenting across the adolescent life span.

North America, Europe, and East Asia); however, research evidence shows that cultural factors may contribute to different parental mediation strategies. For example, Western European parents take more protective approaches, even if it might cost the children online opportunities, while parents of Nordic and northern European countries favor children's rights and freedoms in online environments, even if this may put children at risk.[14] As such, the effectiveness of parental mediation strategies could be different among cultures. Therefore, future work should explore resilience-based adolescent online safety solutions from a global perspective to extend the discussion on adolescent online safety, considering different cultural, legal, and social contexts. This way, teen-centered online safety solutions would be applicable to a wider audience and contribute to a more comprehensive understanding of the issues at hand.

One way to account for these important contextual differences is through teen-centered design that puts teens as the primary stakeholders and authority of their lived digital experiences. By shifting the power dynamic from focusing on the needs and perspectives of parents and adults, amplifying adolescent voices can empower them to learn how to self-regulate their online behaviors in ways that promote resilience, autonomy, and safety. Further, engaging teens as co-designers and researchers can lead to novel design patterns and solutions that will transform the current technology landscape into one that promotes the digital inclusion of teens in the shaping of the platforms in which they engage and the policies put forth to protect them online. Finally, we recognize that resilience-based online safety solutions cannot be considered effective until they have been built, implemented, and evaluated in real-world settings. Therefore, future work to implement the suggested solutions and evaluate them with adolescents in realistic settings is essential. As we do future research with and for adolescents, we must consider ethical responsibilities.

Conducting Ethical and Privacy-Preserving Research With and for Adolescents

Several challenges and ethical considerations surface when conducting online safety and privacy-related research with adolescents. We must ensure that conducting privacy-related research with adolescents does not violate their privacy. For example, power imbalances related to informed consent, data collection, and other aspects of the research process can surface between researchers and adolescents. Since teens are in a developmental stage of transitioning from childhood into adulthood, they are still navigating many physical, cognitive, social, and emotional changes in their bodies. This results in teens being classified as a vulnerable group, requiring several additional protections (e.g., parental consent). However, teens desire individuality, often seeking independence and privacy.

Therefore, Badillo-Urquiola et al.[15] developed a list of heuristic guidelines for conducting risky research with adolescents. These guidelines prioritize the teens' beneficence, autonomy, and privacy, recommending researchers provide teens as much control as possible over how, when, and what types of personal data should be collected. They also encourage the use of help resources, warnings, and disclaimers to support teens before, during, and after participating in a risk-based research study. Legal obligations (e.g., child-mandated abuse reporting) must be clearly communicated to teens in a way that is comprehensible, and expectations of not monitoring data in real time for risk reporting should be clearly stated.

To guide researchers in the United States on best practices for addressing risk mitigation for the protection of youth, Badillo-Urquiola et al. also provided a risk mitigation plan that outlines the ethical considerations and protocols for engaging youth in sensitive and risk-based research. This guide includes ethical considerations beyond the typical U.S. Food and Drug Administration regulations for human subjects research

enforced by institutional review boards. For example, it provides guidance on obtaining a Certificate of Confidentiality from the National Institutes of Health as well as procedures for reporting suspected child abuse or neglect situations. Overall, while we recognize the importance of engaging with teens to design online safety solutions for them, we cannot afford to put them in more danger. Hence, researchers need to prioritize the well-being of teens in conjunction with more research efforts toward establishing best practices and standards for conducting ethical and privacy-preserving research with diverse teens.

In this article, we highlighted a paradigm shift that moves away from restrictive and privacy-invasive strategies toward resilience-based and privacy-preserving solutions to promote adolescent online safety. We also provided an overview of empirical studies that conceptualized and examined various approaches to promoting the digital well-being of teens in a way that empowers teens to be resilient in digital settings. We highlighted a key trend in the emerging literature: teen-centered approaches to promoting digital well-being while supporting the healthy development of adolescents. Empirical evidence increasingly emphasizes that, when it comes to adolescent online safety solutions, the one-size-fits-all approach does not apply. Factors such as age, family context, and culture must be taken into account for online safety solutions that can cater to adolescents with diverse digital experiences and needs. Therefore, we must take a nuanced and contextualized approach to setting a research agenda for the future. Some of the open questions for further exploration around the promotion of adolescents' digital well-being include the following:

- How can we design online safety solutions that can balance protection and support for adolescents' healthy development?
- How can we design online safety solutions for the diversity of adolescents, considering differences in psychological (e.g., child development) and socioecological factors (e.g., family context and cultural norms)?
- How can we implement a comprehensive online protection policy that is respectful of adolescents' digital rights?

Before concluding, we call on a whole village of parents, caregivers, researchers, technology designers/developers, clinicians, educators, and policymakers to put efforts toward positive media parenting and resilience-based approaches to promote the digital well-being of adolescents. Adolescents need guidance from adult actors while they develop a sense of digital autonomy and risk resilience. Hence, an active dialogue between adolescents and supportive adults concerning technology use is key to promoting their digital well-being. Clinicians, educators, and service providers need to support adolescents and caregivers to have healthy conversations about developmentally appropriate parental involvement in their online technology use, focusing on the development of their digital autonomy and resilience. Technology design and development should be evidence based, inclusive, and informed directly by adolescents to ensure that academic research translates into real-world solutions. Finally, comprehensive legislation and policy should be discussed with various stakeholders, including as part of a larger agenda. Adolescent digital privacy needs to be protected as a right, and robust data protection laws for adolescents should be enacted and translated into practice. As such, we call for new practices that push beyond surveillance and restriction toward teen-centric solutions that can best support adolescents' healthy development into digital citizens of the future. ■

Acknowledgment

The work of Dr. Wisniewski was supported by the U.S. National Science Foundation under Grant IIP-2329976, Grant IIS-2333207, and Grant CNS-2326901 and by the William T. Grant Foundation Grant 187941. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the research sponsors.

References

1. M. Anderson, M. Faverio, and J. Gottfried, "Teens, social media and technology 2023." Pewresearch.org. Accessed: Jan. 31, 2024. [Online]. Available: https://www.pewresearch.org/internet/2023/12/11/teens-social-media-and-technology-2023/
2. "S.3663 - Kids Online Safety Act." Congress.gov. Accessed: Jan. 31, 2024. [Online]. Available: https://www.congress.gov/bill/117th-congress/senate-bill/3663/text
3. d.boyd, *It's Complicated: The Social Lives of Networked Teens*. New Haven, CT, USA: Yale Univ. Press, 2014.
4. Z. Iftikhar et al., "Designing parental monitoring and control technology: A systematic review," in *Proc. Human-Comput. Interaction–INTERACT 2021: 18th IFIP TC 13 Int. Conf.*, Bari, Italy. Cham, Switzerland: Springer International Publishing, 2021, pp. 676–700.
5. P. J. Wisniewski, J. Vitak, and H. Hartikainen, "Privacy in adolescence," in *Modern Socio Technical Perspectives on Privacy*, B. P. Knijnenburg, X. Page, P. J. Wisniewski, H. R. Lipford, N. Proferes, J. Romano, eds. Cham, Switzerland: Springer International Publishing, 2022, pp. 315–336.
6. S. Smirnova, S. Livingstone, and M. Stoilova, *Understanding of User Needs and Problems: A Rapid Evidence Review of Age Assurance and Parental Controls*. euConsent. Accessed: May 15, 2024. [Online]. Available: https://eprints.lse.ac.uk/112559/

7. A. K. Ghosh, K. Badillo-Urquiola, S. Guha, J. J. LaViola, Jr, and P. J. Wisniewski, "Safety vs. surveillance: What children have to say about mobile apps for parental control," in *Proc. CHI Conf. Human Factors Comput. Syst. (CHI)*, 2018, pp. 1–14.
8. K. Davis et al., "Supporting Teens' intentional social media use through interaction design: An exploratory proof-of-concept study," in *Proc. 22nd Annu. Conf. ACM Interaction Design Children Conf.*, 2023, pp. 322–334.
9. A. Razi et al., "Instagram data donation: A case study on collecting ecologically valid social media data for the purpose of adolescent online risk detection," in *Proc. CHI Conf. Human Factors Comput. Syst. Extended Abstract (CHI EA)*, 2022, pp. 1–9, doi: 10.1145/3491101.3503569.
10. N. S. Ali, Z. Agha, N. Chatlani, J. Park, and P. J. Wisniewski, "A case study on facilitating a long-term youth advisory board to involve youth in adolescent online safety research," in *Proc. CHI Conf. Human Factors Comput. Syst. Extended Abstract (CHI EA)*, 2024, pp. 1–8, doi: 10.1145/3613905.3637121.
11. Z. Agha et al., "Tricky vs. transparent: Towards an ecologically valid and safe approach for evaluating online safety nudges for teens," in *Proc. CHI Conf. Human Factors Comput. Syst. (CHI)*, 2024, pp. 1–20, doi: 10.1145/3613904.3642313.
12. M. Akter, A. J. Godfrey, J. Kropczynski, H. R. Lipford, and P. J. Wisniewski, "From parental control to joint family oversight: Can parents and teens manage mobile online safety and privacy as equals?," in *Proc. ACM Human-Comput. Interaction*, vol. 6, 2022, pp. 1–28, doi: 10.1145/3512904.
13. K. Badillo-Urquiola, Z. Agha, D. Abaquita, S. B. Harpin, and P. J. Wisniewski, "Towards a social ecological approach to supporting caseworkers in promoting the online safety of youth in foster care," in *Proc. ACM Hum.-Comput. Interaction*, vol. 8, 2024, pp. 135–28, doi: 10.1145/3637412.
14. D. Smahel et al. "EU Kids Online 2020: Survey results from 19 countries." EU KIDS ONLINE. Accessed: May 15, 2024. [Online]. Available: https://eprints.lse.ac.uk/103294/
15. K. Badillo-Urquiola, Z. Shea, Z. Agha, I. Lediaeva, and P. J. Wisniewski, "Conducting risky research with teens: Co-designing for the ethical treatment and protection of adolescents," in *Proc. ACM Hum.-Comput. Interaction*, vol. 4, 2021, pp. 1–46, doi: 10.1145/3432930.

Jinkyung Katie Park is a postdoctoral scholar in computer science at Vanderbilt University, Nashville, TN 37235 USA; she will join the School of Computing at Clemson University as an assistant professor in fall 2024. Her research interests include human–computer interaction, adolescent online safety, and human-centered artificial intelligence. Park received a Ph.D. in information science from Rutgers University. She is an active member of the Association for Computing Machinery Special Interest Group on Computer–Human Interaction, iSchool, and Association for Information Science and Technology communities. Contact her at jinkyung.park@vanderbilt.edu.

Mamtaj Akter is an incoming assistant professor at the New York Institute of Technology, Manhattan, Manhattan, NY 10023 USA. Her research interests include human–computer interaction, adolescent online safety, and usable privacy and security. Akter received a Ph.D. in computer science from Vanderbilt University. She is an active member of the Association for Computing Machinery SIGCHI. Contact her at mamtaj.akter@vanderbilt.edu.

Pamela Wisniewski is an associate professor and a Flowers Family Chancellor Faculty Fellow of Computer Science at Vanderbilt University, Nashville, TN 37235 USA. Her research interests include human–computer interaction, social computing, and adolescent online safety. Wisniewski received a Ph.D. in computer and information systems from the University of North Carolina at Charlotte. She is an Association for Computing Machinery senior member. Contact her at pam.wisniewski@vanderbilt.edu.

Karla Badillo-Urquiola is a Clare Boothe Luce Assistant Professor of Computer Science and Engineering at the University of Notre Dame, Notre Dame, IN 46556 USA. Her current research interests include human–computer interaction, social computing, adolescent online safety, and vulnerable/marginalized populations. Badillo-Urquiola received a Ph.D. in modeling and simulation from the University of Central Florida. She is an active member of the Association for Computing Machinery SIGCHI community. Contact her at kbadillou@nd.edu.