# Towards Resilience and Autonomy-based Approaches for Adolescents Online Safety

Jinkyung Park
*Vanderbilt University*

Mamtaj Akter
*Vanderbilt University*

Naima Samreen Ali
*Vanderbilt University*

Zainab Agha
*Vanderbilt University*

Ashwaq Alsoubai
*Vanderbilt University*

Pamela Wisniewski
*Vanderbilt University*

## Abstract

In this position paper, we discuss the paradigm shift that has emerged in the literature, suggesting to move away from restrictive and authoritarian parental mediation approaches to move toward resilient-based and privacy-preserving solutions to promote adolescents' online safety. We highlight the limitations of restrictive mediation strategies, which often induce a trade-off between teens' privacy and online safety, and call for more teen-centric frameworks that can empower teens to self-regulate while using the technology in meaningful ways. We also present an overview of empirical studies that conceptualized and examined resilience-based approaches to promoting the digital well-being of teens in a way to empower teens to be more resilient.

## 1 Introduction

According to a Pew Research report, 97% 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 use at least one social media platform (95%) [71]. While the majority of U.S. teens shared that being on social media provided them a space for social connection, creativity, and peer support [13], recent research has shown evidence that teens experience many online risks, such as cyberbullying [45], exposure to explicit content [56], problematic internet use with mental health problems (e.g., suicide challenges) [57], and even physical safety risks [69]. Reactions to these new risk experiences were an overemphasis on restrictive and authoritative parental mediation practice [53]. The use of restriction and monitoring by parents may shield teens from online risks, but at the cost of trust between parents and teens, and positive family value as a whole [63, 73]. In this position paper, we discuss the paradigm shift that has emerged in the literature, moving away from restriction and privacy-invasive parental mediation toward resilient-based and privacy-preserving interventions to promote teen online safety. We then provide an overview of empirical studies that our research teams are working on to conceptualize resilience-based approaches to promoting the digital well-being of teens in a way to empower teens to be more resilient. Our position paper is highly relevant to KOPS 2023 as our focus on resilience-based approaches to teen online safety is one of the core topics of interest for KOPS 2023 (i.e., resilience factors associated with minors' crime and safety).

## 2 Background

In this section, we synthesize existing literature that reflects a paradigm shift from emphasizing restrictive monitoring to promoting resilient-based and privacy-preserving approaches to promote teen online safety.

### 2.1 Restriction as a Mean for Protecting Teens from Online Risk

Past literature on parental mediation and adolescent online safety often puts a strong emphasis on abstinence-based strategies (i.e., parental control app) to restrict and monitor teens' online activities [44,64,73]. Through the parental control apps, fine-grained details about teens' smartphone use, such as websites visited, apps installed, calls made, texts sent (including the actual content of the message), and geo-location, are often shared with parents [73]. The rationale behind such tools is to make sure that teens are engaging in age-appropriate ways online and are being sufficiently monitored by their parents when doing so. However, the use of restrictive approaches to monitor their mobile online activities comes with the cost of teens' autonomy [19], trust between parents and teens [72], and positive family value as a whole [73]. More critically, teens such as foster youth are more vulnerable to online risks as they often do not have parents to actively engage with them to ensure their online safety [15, 18].

Social media platforms have also taken restrictive measures to protect youth for instance, by preventing adults from sending private messages to minors they are not connected using sensitivity filters and advanced parental controls [40, 41]. Implementation of such safeguards by social media platforms is grounded by the U.S. federal law, the Children's Online Privacy Protection Act (COPPA) [26], which provided a strong legal ground for the big-tech companies to protect children under 13. Such safeguards, however, do not apply to youth over 13, who have been largely left out of broader public policy debates and self-regulatory industry programs [54].

## 2.2 Trade-offs Between Privacy and Protection

While teens place great social value on their online privacy and appreciate rules and policies that are fair and negotiable [65], as designers and parents, we develop and use surveillance technologies that take teens' privacy away for the sake of their online safety. Scholars, policymakers, security professionals, and advocates have continuously discussed the effects of surveillance/monitoring technologies on individuals and society altogether [21]. In part, complexities and controversies around privacy vs protection discourse are due to a lack of legal frameworks within the U.S. balancing teen online safety and protecting teen privacy rights. Recently, a comprehensive bipartisan legislation, the Kids Online Safety Act (KOSA), has been proposed by U.S. Senators [39]. The legislation requires social media platforms to proactively mitigate harm to minors such as the promotion of self-harm, suicide, and sexual exploitation. It also requires independent audits and public scrutiny from experts to ensure that parents and policymakers know whether social media platforms are taking meaningful steps to address risks to kids [39].

Yet, controversies have continued to rise around KOSA. For instance, teen privacy advocates fear that this legislation would incentivize social media sites to collect *even more information about children* to prevent a set of harms to minors. More importantly, the advocates argued that KOSA could effectively be an instruction for social media platforms to employ a broad range of content filtering to limit minors' access to certain online content, such as sex education for LGBTQ+ youth (which schools had implemented in response to earlier legislation) [30]. Given the repeated failures of social media companies to protect youth from serious risks on their platforms [24, 32, 43], the idea of developing legal frameworks to monitor youth online risk is promising, but only with additional legal safeguards to respect teens' privacy in place. Such legal frameworks are necessary, especially when some of the technical solutions (e.g., AI-based risk detection) rely heavily on teens' intimate data. At the same time, there should be more teen-centric and privacy-preserving solutions that empower teens to self-regulate their online risk experiences and thrive as healthy digital citizens.

## 2.3 Empowering Teens through Resilience-based Interventions and Co-Design with Teens

Teens need autonomy to individuate themselves from their parents, but at the same time, they are less capable than adults at managing online risks without guidance [75]. Hence, there is a need for strength-based design practices that can empower teens and parents to manage online risks in meaningful ways. The key idea around this approach is the paradigm shift from an authoritarian view of protecting teens to more **supportive frameworks that can empower teens to self-regulate and manage technology use in meaningful ways** [35, 75]. In academia, there has been a push for these new approaches respecting teens' rights in the online space, building resilience, and active involvement of both parents and teens to manage teens' online life.

One line of research has conceptualized more collaborative technologies that move away from surveillance-based approaches to ones that engage both teens and parents for digital rule-setting and managing online activities [6, 33, 46, 55]. For instance, Ghosh et al. [36] developed a mobile app that allows adolescents and parents together to negotiate trusted vs. untrusted contact to exchange text messages and confirmed that parents and adolescents who appreciated family values such as privacy, trust, freedom, and balance of power preferred the app over the traditional parental control apps. Another way to support teens' resilience and autonomy is through participatory design that puts teens as the primary stakeholder and authority of their own online experiences. Co-design research with teens has been successful in including teen voices and their unique perspectives to design resilience-based approaches for promoting their online safety [3, 14, 61]. By giving voice to the design process of their online safety solutions, teens can reflect on their own online habits and learn how to self-regulate such habits in ways that promote resilience, autonomy, and digital well-being [23].

# 3 Research on Resilience-based Approaches to Support Teen Online Safety

Over the past decade, our research team has been working on several research projects related to the topic of adolescents' online safety and risks [1, 3–6, 10–12, 15–17, 23, 33–36, 59, 61, 62]. In this section, we will summarize how our ongoing research moves beyond traditional approaches relying on unidirectional 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.

### 3.1 Youth Advisory Board/Teenovate

Teen-centered Participatory Design (PD) programs have made successful efforts in involving teens directly in the design process of online safety interventions [3, 23]. Still, the current PD practices are found to be insufficient in retaining teen participants who may not find the program rewarding enough, or perceive power imbalances between themselves and adult researchers pertaining to knowledge gaps [28, 58]. Therefore, the authors engaged 21 teens to plan and develop Teenovate Youth Advisory Board (YAB) [23], a longitudinal participatory action research program for teens. In YAB, teens act as co-researchers to give feedback on the proposed adolescent online safety research and do design activities to promote their own online safety. Through the participatory sessions, YAB teens provided us with insights such as how to improve the working relationships with teen participants or behavioral approaches for resolving possible conflicts between teens and adult researchers. Additionally, YAB offers training workshops focused on human-centered research and User Experience (UX), to equip teens with the necessary tools to make strides and effectively contribute to designing various solutions for their safety online.

With the YAB members, the authors have also explored the potential of the Asynchronous Research Community (ARC) [49] methodology to improve engagement by encouraging them to post discussion comments and interact with peer participants and researchers on topics related to adolescent online safety research on Discord [42]. Through the ARC study, the authors found that teens are most interested in exploring topics related to their online privacy on social media. YAB teens shared that they consciously decide which social media platforms to use depending on their user goals (e.g., content viewing or socializing), and employ varied strategies to strike a balance between meeting their goals and mitigating privacy risks. The findings suggest that understanding teens' motivations and needs for social media use and their differing privacy perceptions is pivotal to providing them with customized support systems for safer online experiences [42].

One of the key lessons learned from the YAB teens was that teens consider the co-design sessions as an opportunity to channel their creativity skills and online experiential knowledge to devise tangible solutions for their online safety. They also found benefits of participating in adolescent online safety research as it allowed them to reflect on their own online interactions and reconsider the online safety measures that would work best for them. Overall, participating in co-design activities helped teens feel more confident and empowered to contribute freely to the research aimed at promoting their online safety. In the future, these insights will serve as the guiding beacon to generate study design patterns for researchers suggesting best practices to conduct online safety research for teens with teens.

### 3.2 Joint Family Oversight for Adolescents' Mobile Online Safety, Security and Privacy

In families, parents often use parental monitoring or controlling apps to ensure their teens' mobile online safety. However, teens often find this constant surveillance overly restrictive and privacy-invasive, affecting parent-teen relationships [34, 74]. Therefore, adolescents online safety researchers have called for adopting more collaborative [27, 38, 47] and teen-centric approaches where teens can have some level of privacy and autonomy in their own online safety [22, 36]. In an attempt to move toward more bi-directional approaches for mobile online safety, Akter et al. [6] leveraged the concepts of the community oversight model for privacy and security [25] and developed a joint family oversight mechanism, titled CO-oPS [4, 7], to help parents and teens collaboratively manage their mobile privacy, online safety, and security. This CO-oPS app provided a transparent view of one another's apps installed and the privacy permissions granted or denied to the apps and allowed to provide direct feedback to one another, facilitating more parent-teen communication. However, it also allows users to manage the level of transparency by allowing them to hide any of the apps installed that they do not want to be shared with other users.

Through a lab-based study with 19 parent-teen dyads, Akter et al. [6] evaluated the CO-oPS app to assess whether it would be useful for their families in managing mobile online safety, security, and privacy. They found that even though teens were the primary tech support providers in the family, parents were concerned for their teens' mobile online safety and, therefore, often manually checked their phones to review the apps installed or used parental control apps to restrict new app installation. In evaluating the CO-oPS app, both parents and teens found value in the feature that allowed them to review one another's apps and permissions, as it increased the transparency of their app usage and helped initiate more discussion around mobile privacy and security. The authors also observed that parents were more concerned about teens' app usage, seeing them as access points to their children by others online. In contrast, teens mostly focused on the permissions granted on their parent's phones, being more aware of the malicious intent of third-party mobile apps. However, they also found that such bidirectional co-monitoring made parents uncomfortable relinquishing control over their teens. In contrast, teens felt it was not their place to oversee their parents' mobile privacy and security.

Overall, Akter et al. [6] demonstrated that by encouraging more collaborative monitoring and communication, bidirectional oversight between parents and adolescents might potentially increase families' overall knowledge and awareness of mobile privacy, security, and online safety, which they further confirmed in a later study [5]. However, for these beneficial results to take place, both parents and adolescents must agree that it is their responsibility to look out for one another, which requires a significant paradigm shift from the adolescent online safety approaches that have been predominantly used in our society. Additionally, the insights derived from employing CO-oPS within family contexts [6] can offer advantages not only to designers developing similar joint family online safety tools but also to designers creating strategies aimed at assisting users in safeguarding their digital privacy. This extends beyond the domain of mobile online safety to encompass broader areas of digital privacy and security, including smart home devices [8, 9, 29], social media [20, 66, 68, 70], websites [51, 52], and other platforms where teenagers and their families share personal information with third parties.

## 3.3 Youth-centered Online Risk Detection

Computational approaches to identify teen online risk have been applied as promising alternatives for human labor to do the same tasks, given the scale of online content. Yet, a common trend among these approaches is a lack of teen-centered aspects [11, 45, 62], such as a lack of understanding of the context of risks teens experience [12]. In this study, the focus was to improve our understanding of teens' online risk experiences across online and offline contexts by aligning their self-reported surveys with explicit risk flagging, the evidence of which can help provide youth more agency for their online/offline safety. In this IRB-approved user study, the authors worked with 173 youths (ages 13-21) to collect self-reported surveys regarding their online and offline risk experiences. Then, youths were asked to upload their private social media (i.e., Instagram Direct Messages) data to self-assess the risks in their private conversations (e.g., risk type, level of risk, etc.) [60]. The authors created profiles of youth based on their self-reported survey data and compared the profiles with the risk type and levels that the youth flagged. Five unique profiles of youth emerged: 1) Low Risks, 2) Medium Risks, 3) Increased Sexting, 4) Increased Self-Harm, and 5) High-Risk Perpetration.

The comparative analysis confirmed that youth self-reported online and offline risk experiences were fairly aligned with their social media trace data and that youth risk experiences varied depending on their profiles. For instance, while youths in the low-Risk group were exposed to spam and scam messages and the self-harm disclosures of others, those in the medium-risk group mostly encountered harassment. Another key finding was the mismatch between offline and online risk contexts. For example, youth in the Increased Self-Harm profile group reported the highest levels of offline self-harm, but their unsafe conversations did not contain digital self-harm content; instead, they engaged in more unsafe sexual conversations. The results of the study highlighted the importance of understanding the multidimensionality of youth online risk experience as it is pivotal for designing youth-centric and customized risk prevention strategies to promote youth resilience from online risk. More importantly, having such in-depth knowledge of youth online risk experience is critical to inform the design and development of youth-centered computational systems to identify nuanced and contextualized online harms that youth experience at scale. Based on the knowledge gained from this study, the authors are working on designing youth-centered "real-time" risk detection models as 'just-in-time' interventions to mitigate their online risk experience.

## 3.4 Real-time Nudge-based Intervention

"Nudges" are subtle cues that aim to influence people's behavior without compromising their decision-making autonomy [67] and have been proposed as a 'just-in-time' intervention to support teens at the moment when they experience risks online [1, 3]. Yet, a majority of the prior work within the online safety space has focused more on *designing* interventions [17, 37], with less realistic evaluations to assess the effectiveness nudges for teen online safety. Moreover, the few evaluations of adolescent online safety interventions have relied on self-reported survey-based feedback [50], which is subject to recall bias and does not provide an ecologically valid setting for evaluations. To overcome this, one way for evaluating nudges is by simulating the environment and risks to understand how nudges lead to actual behavior change for adolescent online safety. Such simulation-based evaluations have been studied as a promising approach within other related fields of privacy and security [48, 76]. In order to design realistic bad actors and risk scenarios for nudge evaluation within a Social Media Simulation, it is crucial to involve teens in designing such a simulated environment.

Therefore, the authors conducted co-design sessions with 14 teens (13-18 years old) in the United States to obtain their feedback on the design of user personas and risk scenarios which will be implemented in a social media simulation, for evaluating adolescents' online safety interventions [2]. During these sessions, the authors presented teens with 10 prepared user personas and 4 risky scenarios based on prior research [1]. Teens redesigned various aspects of the social media personas and scenarios using an online whiteboard tool, FigJam [31]. The results show that teens considered the characteristics of the risky user to be important and designed personas to have traits that align with the risk type, were more believable and authentic, and attracted teens through materialistic content. Teens also redesigned the risky scenarios to be subtle in information breaching, harsher in cyberbullying, and convincing in tricking the teen. The findings from the co-design sessions emphasized the importance of designing simulations that are sensitive to the needs and perspectives of teens and that provide a nuanced and realistic environment for evaluating online safety interventions [2]. Moving forward, the authors are planning to implement the designs from this study in a between-subjects experimental design with teens to evaluate the effectiveness of the different types of nudges within a social media simulation.

## 4 Conclusion

In this position paper, we highlighted a paradigm shift that has emerged in the literature in a way that moves away from restriction and authoritarian parental mediation toward resilient-based and privacy-preserving solutions to promote teen 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 to empower teens to be more resilient. A common theme among the studies that we introduced above is a call for teen-centered approaches to promoting teens' digital well-being while supporting the healthy development of teens. As many of the studies are ongoing projects, more empirical evidence of the benefits of resilience-based interventions will be documented. Having said that, participating in KOPS 2023 would be extremely beneficial for us to share ongoing projects and have interactive feedback from the workshop participants, which could potentially lead to more collaboration opportunities. Finally, we anticipate learning more about others' translational research to promote teen resilience by participating in the workshop.

## References

[1] Zainab Agha, Karla Badillo-Urquiola, and Pamela J Wisniewski. " strike at the root": Co-designing real-time social media interventions for adolescent online risk prevention. *Proceedings of the ACM on Human-Computer Interaction*, 7(CSCW1):1–32, 2023.

[2] Zainab Agha, Kelsey Miu, Sophia Piper, Jinkyung Park, and Pamela J Wisniewski. Co-designing user personas and risk scenarios for evaluating adolescent online safety interventions. In *Computer Supported Cooperative Work and Social Computing*, pages 249–253. 2023.

[3] Zainab Agha, Zinan Zhang, Oluwatomisin Obajemu, Luke Shirley, and Pamela J. Wisniewski. A case study on user experience bootcamps with teens to co-design real-time online safety interventions. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, pages 1–8, 2022.

[4] Mamtaj Akter, Leena Alghamdi, Dylan Gillespie, Nazmus Sakib Miazi, Jess Kropczynski, Heather Lipford, and Pamela J. Wisniewski. Co-ops: A mobile app for community oversight of privacy and security. In *Companion Publication of the 2022 Conference on Computer Supported Cooperative Work and Social Computing*, CSCW'22 Companion, page 179–183, New York, NY, USA, 2022. Association for Computing Machinery.

[5] Mamtaj Akter, Leena Alghamdi, Jess Kropczynski, Heather Richter Lipford, and Pamela J. Wisniewski. It takes a village: A case for including extended family members in the joint oversight of family-based privacy and security for mobile smartphones. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI EA '23, Hamburg, Germany, 2023. Association for Computing Machinery.

[6] Mamtaj Akter, Amy J Godfrey, Jess Kropczynski, Heather R Lipford, and Pamela J Wisniewski. From parental control to joint family oversight: Can parents and teens manage mobile online safety and privacy as equals? *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW1):1–28, 2022.

[7] Mamtaj Akter, Madiha Tabassum, Nazmus Sakib Miazi, Leena Alghamdi, Jess Kropczynski, Pamela J. Wisniewski, and Heather Lipford. Evaluating the impact of community oversight for managing mobile privacy and security. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, pages 437–456, Anaheim, CA, August 2023. USENIX Association.

[8] Leena Alghamdi, Mamtaj Akter, Cristobal Sepulveda Cardenas, Diego A. Cruces, Jason Wiese, Jess Kropczynski, Heather Lipford, and Pamela J. Wisniewski. Mi casa es su casa ("misu"): A mobile app for sharing smart home devices with people outside the home. In *Companion Publication of the 2022 Conference on Computer Supported Cooperative Work and Social Computing*, CSCW'22 Companion, page 184–187, New York, NY, USA, 2022. Association for Computing Machinery.

[9] Leena Alghamdi, Mamtaj Akter, Jess Kropczynski, Pamela J. Wisniewski, and Heather Lipford. Co-designing community-based sharing of smarthome devices for the purpose of co-monitoring in-home emergencies. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery.

[10] Ashwaq Alsoubai. A human-centered approach to improving adolescent real-time online risk detection algorithms. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI EA '23, New York, NY, USA, 2023. Association for Computing Machinery.

[11] Ashwaq Alsoubai, Xavier V. Caddle, Ryan Doherty, Alexandra Taylor Koehler, Estefania Sanchez, Munmun De Choudhury, and Pamela J. Wisniewski. Mosafely, is that sus? a youth-centric online risk assessment dashboard. In *Companion Publication of the 2022 Conference on Computer Supported Cooperative Work and Social Computing*, CSCW'22 Companion, page 197–200,

New York, NY, USA, 2022. Association for Computing Machinery.

[12] Ashwaq Alsoubai, Jihye Song, Afsaneh Razi, Nurun Naher, Munmun De Choudhury, and Pamela J. Wisniewski. From 'friends with benefits' to 'sextortion:' a nuanced investigation of adolescents' online sexual risk experiences. *Proc. ACM Hum.-Comput. Interact.*, 6(CSCW2), nov 2022.

[13] Monica Anderson, Emily A Vogels, Andrew Perrin, and Lee Raine. Connection, creativity and drama: Teen life on social media in 2022, 2022.

[14] Zahra Ashktorab and Jessica Vitak. Designing cyberbullying mitigation and prevention solutions through participatory design with teenagers. In *Proceedings of the 2016 CHI conference on human factors in computing systems*, pages 3895–3905, 2016.

[15] Karla Badillo-Urquiola, Scott Harpin, and Pamela Wisniewski. Abandoned but not forgotten: Providing access while protecting foster youth from online risks. In *Proceedings of the 2017 Conference on Interaction Design and Children*, pages 17–26, 2017.

[16] Karla Badillo-Urquiola, Xinru Page, and Pamela J Wisniewski. Risk vs. restriction: The tension between providing a sense of normalcy and keeping foster teens safe online. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2019.

[17] Karla Badillo-Urquiola, Diva Smriti, Brenna McNally, Evan Golub, Elizabeth Bonsignore, and Pamela J Wisniewski. Stranger danger! social media app features co-designed with children to keep them safe online. In *Proceedings of the 18th ACM International Conference on Interaction Design and Children*, pages 394–406, 2019.

[18] Karla A Badillo-Urquiola, Arup Kumar Ghosh, and Pamela Wisniewski. Understanding the unique online challenges faced by teens in the foster care system. In *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, pages 139–142, 2017.

[19] Diana Baumrind. Patterns of parental authority and adolescent autonomy. *New directions for child and adolescent development*, 2005(108):61–69, 2005.

[20] Sruti Bhagavatula, Lujo Bauer, and Apu Kapadia. "adulthood is trying each of the same six passwords that you use for everything": The scarcity and ambiguity of security advice on social media. *Proc. ACM Hum.-Comput. Interact.*, 6(CSCW2), nov 2022.

[21] Johann Čas, Rocco Bellanova, J Peter Burgess, Michael Friedewald, and Walter Peissl. Introduction: Surveillance, privacy and security. In *Surveillance, Privacy and Security*, pages 1–12. Routledge, 2017.

[22] Markos Charalambous, Petros Papagiannis, Antonis Papasavva, Pantelitsa Leonidou, Rafael Constaninou, Lia Terzidou, Theodoros Christophides, Pantelis Nicolaou, Orfeas Theofanis, George Kalatzantonakis, and Michael Sirivianos. A Privacy-Preserving Architecture for the Protection of Adolescents in Online Social Networks. *arXiv:2007.12038 [cs]*, July 2020. arXiv: 2007.12038.

[23] Neeraj Chatlani, Arianna Davis, Karla Badillo-Urquiola, Elizabeth Bonsignore, and Pamela Wisniewski. Teen as research-apprentice: A restorative justice approach for centering adolescents as the authority of their own online safety. *International Journal of Child-Computer Interaction*, 35:100549, 2023.

[24] Neha Chaudhary and Nina Vasan. 3 ways for big tech to protect teens from harm, 2020.

[25] Chhaya Chouhan, Christy M. LaPerriere, Zaina Aljallad, Jess Kropczynski, Heather Lipford, and Pamela J. Wisniewski. Co-designing for Community Oversight: Helping People Make Privacy and Security Decisions Together. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–31, November 2019.

[26] Federal Trade Commission. Children's online privacy protection rule, January 2013.

[27] Lorrie Faith Cranor, Adam L. Durity, Abigail Marsh, and Blase Ur. Parents' and Teens' Perspectives on Privacy In a Technology-Filled World. pages 19–35, 2014.

[28] Arianna J Davis. Co-designing" teenovate": An intergenerational online safety design team. 2020.

[29] Pardis Emami Naeini, Martin Degeling, Lujo Bauer, Richard Chow, Lorrie Faith Cranor, Mohammad Reza Haghighat, and Heather Patterson. The influence of friends and experts on privacy decision making in iot scenarios. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), nov 2018.

[30] Lauren Feiner. Kids online safety act may harm minors, civil society groups warn lawmakers, 2022.

[31] Figma. Figjam turn possibilities into plans, 2023.

[32] Brian Fung. Senators blast big tech companies over kids' safety amid renewed push for legislation, 2023.

[33] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J LaViola Jr, and Pamela J Wisniewski. Safety vs. surveillance: what children have to say about

mobile apps for parental control. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2018.

[34] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J. LaViola Jr, and Pamela J. Wisniewski. Safety vs. Surveillance: What Children Have to Say about Mobile Apps for Parental Control. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, pages 1–14, New York, NY, USA, April 2018. Association for Computing Machinery.

[35] Arup Kumar Ghosh, Karla Badillo-Urquiola, Mary Beth Rosson, Heng Xu, John M Carroll, and Pamela J Wisniewski. A matter of control or safety? examining parental use of technical monitoring apps on teens' mobile devices. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2018.

[36] Arup Kumar Ghosh, Charles E. Hughes, and Pamela J. Wisniewski. Circle of Trust: A New Approach to Mobile Online Safety for Families. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–14, Honolulu HI USA, April 2020. ACM.

[37] Heidi Hartikainen, Netta Iivari, and Marianne Kinnula. Children's design recommendations for online safety education. *International Journal of Child-Computer Interaction*, 22:100146, 2019.

[38] Yasmeen Hashish, Andrea Bunt, and James E. Young. Involving children in content control: a collaborative and education-oriented content filtering approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, pages 1797–1806, New York, NY, USA, April 2014. Association for Computing Machinery.

[39] https://www.blumenthal.senate.gov/. Blumenthal & blackburn introduce comprehensive kids' online safety legislation, 2022.

[40] Instagram. Continuing to make instagram safer for the youngest members of our community, 2021.

[41] Instagram. Introducing sensitive content control, 2021.

[42] Naulsberry Jean Baptiste, Jinkyung Park, Neeraj Chatlani, Naima Samreen Ali, and Pamela J Wisniewski. Teens on tech: Using an asynchronous remote community to explore adolescents' online safety perspectives. In *Computer Supported Cooperative Work and Social Computing*, pages 45–49. 2023.

[43] The Wall Street Journal. the facebook files a wall street journal investigation, 2023.

[44] Atika Khurana, Amy Bleakley, Amy B Jordan, and Daniel Romer. The protective effects of parental monitoring and internet restriction on adolescents' risk of online harassment. *Journal of youth and Adolescence*, 44:1039–1047, 2015.

[45] Seunghyun Kim, Afsaneh Razi, Gianluca Stringhini, Pamela J Wisniewski, and Munmun De Choudhury. A human-centered systematic literature review of cyberbullying detection algorithms. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–34, 2021.

[46] Minsam Ko, Seungwoo Choi, Subin Yang, Joonwon Lee, and Uichin Lee. Familync: facilitating participatory parental mediation of adolescents' smartphone use. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 867–878, 2015.

[47] Jess Kropczynski, Reza Ghaiumy Anaraky, Mamtaj Akter, Amy J. Godfrey, Heather Lipford, and Pamela J. Wisniewski. Examining collaborative support for privacy and security in the broader context of tech caregiving. *Proc. ACM Hum.-Comput. Interact.*, 5(CSCW2), oct 2021.

[48] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. Teaching johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, 10(2):1–31, 2010.

[49] Haley MacLeod, Ben Jelen, Annu Prabhakar, Lora Oehlberg, Katie A Siek, and Kay Connelly. Asynchronous remote communities (arc) for researching distributed populations. In *PervasiveHealth*, pages 1–8, 2016.

[50] Hiroaki Masaki, Kengo Shibata, Shui Hoshino, Takahiro Ishihama, Nagayuki Saito, and Koji Yatani. Exploring nudge designs to help adolescent sns users avoid privacy and safety threats. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–11, 2020.

[51] Nora McDonald and Helena M. Mentis. Building for 'we': Safety settings for couples with memory concerns. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[52] Nora Mcdonald and Helena M. Mentis. "citizens too": Safety setting collaboration among older adults with memory concerns. *ACM Trans. Comput.-Hum. Interact.*, 28(5), aug 2021.

[53] Kathryn L. Modecki, Rachel E. Goldberg, Pamela Wisniewski, and Amy Orben. What is digital parenting? a systematic review of past measurement and blueprint for the future. *Perspectives on Psychological Science*, 17(6):1673–1691, 2022.

[54] Kathryn C Montgomery. Youth and surveillance in the facebook era: Policy interventions and social implications. *Telecommunications Policy*, 39(9):771–786, 2015.

[55] Marije Nouwen, Nassim JafariNaimi, and Bieke Zaman. Parental controls: reimagining technologies for parent-child interaction. In *Proceedings of 15th European Conference on Computer-Supported Cooperative Work-Exploratory Papers*, volume 2017, pages 18–34. European Society for Socially Embedded Technologies (EUSSET), 2017.

[56] Jinkyung Park, Joshua Gracie, Ashwaq Alsoubai, Gianluca Stringhini, Vivek Singh, and Pamela Wisniewski. Towards automated detection of risky images shared by youth on social media. In *Companion Proceedings of the ACM Web Conference 2023*, pages 1348–1357, 2023.

[57] Jinkyung Park, Irina Lediaeva, Maria Lopez, Amy Godfrey, Kapil Chalil Madathil, Heidi Zinzow, and Pamela Wisniewski. How affordances and social norms shape the discussion of harmful social media challenges on reddit. *Human Factors in Healthcare*, 3:100042, 2023.

[58] Erika S Poole and Tamara Peyton. Interaction design research with adolescents: methodological challenges and best practices. In *Proceedings of the 12th International Conference on Interaction Design and Children*, pages 211–217, 2013.

[59] Afsaneh Razi. Deploying human-centered machine learning to improve adolescent online sexual risk detection algorithms. In *Companion of the 2020 ACM international conference on supporting group work*, pages 157–161, 2020.

[60] Afsaneh Razi, Ashwaq Alsoubai, Seunghyun Kim, Nurun Naher, Shiza Ali, Gianluca Stringhini, Munmun De Choudhury, and Pamela J. Wisniewski. Instagram data donation: A case study on collecting ecologically valid social media data for the purpose of adolescent online risk detection. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI EA '22, New York, NY, USA, 2022. Association for Computing Machinery.

[61] Afsaneh Razi, Karla Badillo-Urquiola, and Pamela J Wisniewski. Let's talk about sext: How adolescents seek support and advice about their online sexual experiences. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2020.

[62] Afsaneh Razi, Seunghyun Kim, Ashwaq Alsoubai, Gianluca Stringhini, Thamar Solorio, Munmun De Choudhury, and Pamela J Wisniewski. A human-centered systematic literature review of the computational approaches for online sexual risk detection. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–38, 2021.

[63] Tara L Rutkowski, Heidi Hartikainen, Kirsten E Richards, and Pamela J Wisniewski. Family communication: Examining the differing perceptions of parents and teens regarding online safety communication. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–23, 2021.

[64] Diane J Schiano and Christine Burg. Parental controls: Oxymoron and design opportunity. In *HCI International 2017–Posters' Extended Abstracts: 19th International Conference, HCI International 2017, Vancouver, BC, Canada, July 9–14, 2017, Proceedings, Part II 19*, pages 645–652. Springer, 2017.

[65] Valerie Steeves and Priscilla Regan. Young people online and the social value of privacy. *Journal of Information, Communication and Ethics in Society*, 2014.

[66] Jose M. Such and Michael Rovatsos. Privacy policy negotiation in social media. *ACM Trans. Auton. Adapt. Syst.*, 11(1), feb 2016.

[67] Richard H Thaler and Cass R Sunstein. *Nudge: Improving decisions about health, wealth, and happiness*. Penguin, 2009.

[68] Onuralp Ulusoy and Pinar Yolum. Panola: A personal assistant for supporting users in preserving privacy. *ACM Trans. Internet Technol.*, 22(1), sep 2021.

[69] Patti M Valkenburg, Adrian Meier, and Ine Beyens. Social media use and its impact on adolescent mental health: An umbrella review of the evidence. *Current opinion in psychology*, 44:58–68, 2022.

[70] Nishant Vishwamitra, Yifang Li, Kevin Wang, Hongxin Hu, Kelly Caine, and Gail-Joon Ahn. Towards pii-based multiparty access control for photo sharing in online social networks. In *Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies*, SACMAT '17 Abstracts, page 155–166, New York, NY, USA, 2017. Association for Computing Machinery.

[71] Emily A Vogels, Risa Gelles-Watnick, and Navid Massarat. Teens, social media and technology 2022, 2022.

[72] Angie Williams. Adolescents' relationships with parents. *Journal of language and social psychology*, 22(1):58–65, 2003.

[73] Pamela Wisniewski, Arup Kumar Ghosh, Heng Xu, Mary Beth Rosson, and John M Carroll. Parental control vs. teen self-regulation: Is there a middle ground for mobile online safety? In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, pages 51–69, 2017.

[74] Pamela Wisniewski, Arup Kumar Ghosh, Heng Xu, Mary Beth Rosson, and John M. Carroll. Parental control vs. teen self-regulation: Is there a middle ground for mobile online safety? In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, CSCW '17, page 51–69, New York, NY, USA, 2017. Association for Computing Machinery.

[75] Pamela J Wisniewski, Jessica Vitak, and Heidi Hartikainen. Privacy in adolescence. In *Modern Socio-Technical Perspectives on Privacy*, pages 315–336. Springer International Publishing Cham, 2022.

[76] Maximilian Zinkus, Oliver Curry, Marina Moore, Zachary Peterson, and Zoë J Wood. Fakesbook: A social networking platform for teaching security and privacy concepts to secondary school students. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*, pages 892–898, 2019.