Privacy Challenges for Adolescents as a Vulnerable Population

Afsaneh Razi
University of Central Florida
Orlando, FL USA
Afsaneh.razi@Knights.ucf.edu

Pamela Wisniewski
University of Central Florida
Orlando, FL USA
pamwis@ucf.edu

Zainab Agha
University of Central Florida
Orlando, FL USA
zainab.agha@Knights.ucf.edu

Neeraj Chatlani
University of Central Florida
Orlando, FL USA
nchatlani@Knights.ucf.edu

Abstract
Future online safety technologies should consider the privacy needs of adolescents (ages 13-17) and support their ability to self-regulate their online behaviors and navigate online risks. To do this, adolescent online safety researchers and practitioners must shift towards solutions that are more teen-centric by designing privacy-preserving online safety solutions for teens. In this paper, we discuss privacy challenges we have encountered in conducting adolescent online safety research. We discuss privacy concerns of teens in regard to sharing their private social media data with researchers and potentially taking part in a user study where they share some of this information with their parents. Our research emphasizes a need for more privacy-preserving interventions for teens.

Author Keywords
Privacy; Adolescent Online Safety; Vulnerable Population.

ACM Classification Keywords
• Human-centered computing~HCI theory, concepts and models • Security and privacy → Human and societal aspects of security and privacy

Motivation and Background
Internet and social media are present in the lives of teenagers more than ever; according to Pew Research,

92% of teens ages 13 to 17 go online daily, 73% have access to mobile smartphones, and 71% engage on more than one social media platform in the USA [6]. While staying connected via social media and smartphones has its own merits, it also intensifies online risks. As it is reported in Crimes against Children Research Center, 23% of youth have experienced unwanted exposure to Internet pornography, 11% have been victims of online harassment, and 9% report receiving unwanted sexual solicitations online [5].

For protecting teens online, past research aimed at increasing teens' awareness of privacy with this assumption that adolescents take poor privacy decisions due to their lack of concerns [3]. This notion has resulted in online safety tools that allow parents to monitor and restrict their teen's online presence [9]. This privacy-invasive approach exacerbates the tensions between parents and teens [10]. Past literature shows that restrictive approaches have a suppressive effect and do not teach teens how to effectively protect themselves online [11]. Wisniewski et al. call for more teen-centric approaches than parent-centric approaches that consider teens' needs as the primary stakeholders [9]. For instance, researchers found that online sexual interactions have become a normal part of adolescents' lives, which they are seeking support online about how to address them [8]. This demonstrates that adolescents are seeking support beyond their families to receive support for their online interactions.

Pinter et al. raise the concern that in the area of adolescent online safety, most research uses teens' self-reported data which might not reflect the actual teens' online behaviors [7]. As self-reported data are prone to different types of biases such as recall or social desirability biases [4], our aim is to go beyond self-reported data by investigating teens' social media data. One of the reasons that current technical interventions are not helpful for teens and parents is that they do not take to account the context in which these online risky interactions occur. Therefore, we aim to take into consideration teens' privacy and create solutions that situate the context based on their social media data in which these risks happen.

Privacy Challenges for Research for Adolescent Online Safety

We are in the process of conducting an NSF-funded research project [12] to improve teens' online safety by using human-centered machine learning on their real social media data. We are using these methods to improve online risk detection algorithms which can be used in more privacy-preserving online safety systems. This project includes two phases. In the first phase, teens and young adults would answer questions about their online and personal experiences and will then be asked to upload their Instagram data to our website. Our aim is to understand the online risk perceptions of teens about their own social media data. This would be used to create a dataset. In the second phase, teens flag their Instagram private messages for risky encounters, and then participate in a discussion exercise with parents, based on these instances.

In the first phase, we are trying to bridge the gap between qualitative and computational approaches. For developing fair and helpful machine learning algorithms, robust training datasets that are based on teens' actual social media are needed. The qualitative approaches will be used to create risk models of teens'

online experiences to address their needs. Then the social media of the teen would be labeled on the riskiness of the information and this training dataset will be used for developing machine learning approaches. In the second phase, we want to understand different perceptions about online risks from parents and teens and help them reconcile these discrepancies. So, we can form a consensus about what risks are the most salient ones to address in our research. In the next section, we discuss the privacy challenges of doing this research project from an initial study with youth.

Considering Privacy When Collecting Sensitive Data
In order to gain insight into the privacy needs of teens regarding sharing and discussing sensitive data, we conducted semi-structured interviews with 10 undergraduate students [1], who represent the unique perspective of "emerging adults" [2] that are past adolescence but not yet adults. We sought to have our participants provide their thoughts on how to best balance tensions with parents and teens when having conversations about sensitive social media messages, while also preserving the teen's sense of privacy and control over their data.

One of the biggest concerns shared by our participants was the need for privacy and protection of the social media data itself. Specific concerns included the inclusion of non-risky, personal interactions alongside the highlighted risky instances, and the privacy of their friends and others involved in their private messages. Additionally, participants wanted control over the data that was shared with parents for the purpose of discussion. They recommended selectively sharing data with parents, excluding intimate personal interactions, or anonymizing the messages. Another common suggestion was to have the parent-teen discussion based on social media data that was not their own.

The key take-away from our findings was the need to ensure that teens have full agency over how their social media data is shared and used by researchers, especially when the study concerns messages of a sensitive nature. In terms of how researchers use the data, having explicit details in participants' consent forms over how their data will be disseminated would help put them more at ease when deciding whether to consent to the study. Furthermore, to ensure that teens are not later harmed by sharing any of their data with us, we have obtained an NIH Certificate of Confidentiality [13], which protects their information from being shared with other parties without their express permission, including safeguarding it from being subpoenaed for legal purposes.

To protect our participants when faced with the task of discussing their sensitive social media messages with parents, we make several provisions in the design of our study. First, we explicitly anonymize all other parties in private messages, besides the teen's messages. Second, we give the teen control over which messages excerpts are shared with parents, additionally allowing them to anonymize their own messages if they so choose. Finally, in the case that teens are not at all comfortable with the idea of discussing their private messages with their parents, we allow them to share their social media data with the researchers and then opt out of the discussion-based exercise with their parents.

Conclusion

We have identified some key challenges in balancing the tensions between online safety and privacy for teens and presented some solutions to overcome these challenges. For designing and developing more teen-centric approaches, there is a need for more investigation on teens' privacy perceptions while providing them safe online environments. It would be of a great benefit if privacy researchers would discuss these challenges ahead of teens' online safety. The Privacy and Power workshop at CHI 2020 would provide a great venue to discuss the unique needs and challenges of privacy for vulnerable populations, and we hope to gain more insight about possible solutions on how to address these challenges.

Afsaneh Razi is a Ph.D. candidate in the Department of Computer Science at the University of Central Florida. She is a member of the Socio-Technical Interaction Research (STIR) Lab at UCF. Her current research is to improve adolescent online safety utilizing human-centered machine learning approaches. This is part of an NSF funded project to improve online risk detection algorithms for adolescent.

Zainab Agha is a Ph.D. student in the Department of Computer Science at the University of Central Florida. She is working on projects focusing on adolescent online safety at the STIR Lab. Her current research takes a teen-centric approach to online safety, aiming to reduce tensions between parents and teens regarding their perceptions of online risks.

Neeraj Chatlani is a Ph.D. student in the Department of Computer Science at the University of Central Florida, working within the STIR Lab. His current work involves the creation of risk models of teen online interaction, and the use of participatory design to engage teens in the creation of online safety strategies.

Pamela J. Wisniewski is the Director of the STIR Lab and an Assistant Professor in the Department of Computer Science at the University of Central Florida. Her work lies at the intersection of Social Computing and Privacy. She is an expert in the interplay between social media, privacy, and online safety for adolescents, particularly at-risk teens who are most vulnerable to serious online risks.

Acknowledgements

This research is partially supported by the U.S. National Science Foundation under grants IIP-1827700 and IIS-1844881, and by the William T. Grant Foundation grant #187941. Any opinions, findings, and 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] Zainab Agha, Neeraj Chatlani, Afsaneh Razi, and Pamela Wisniewski. Towards Conducting Responsible Research with Teens and Parents regarding Online Risks. In *CHI 2020 Extended Abstracts*. https://doi.org/10.1145/3334480.3383073

[2] J. J. Arnett. 2000. Emerging adulthood. A theory of development from the late teens through the twenties. *The American Psychologist* 55, 5: 469–480.

[3] Susan Barnes. 2006. A Privacy Paradox: Social networking in the United States. *First Monday* 11. https://doi.org/10.5210/fm.v11i9.1394

[4] Robert J. Fisher. 1993. Social Desirability Bias and the Validity of Indirect Questioning. *Journal of Consumer Research* 20, 2: 303–315. https://doi.org/10.1086/209351

[5] Lisa M. Jones, Kimberly J. Mitchell, and David Finkelhor. 2012. Trends in Youth Internet Victimization: Findings From Three Youth Internet Safety Surveys 2000–2010. *Journal of Adolescent Health* 50, 2: 179–186. https://doi.org/10.1016/j.jadohealth.2011.09.015

[6] Amanda Lenhart, Monica Anderson, and Aaron Smith. 2015. Teens, Technology and Romantic Relationships | Pew Research Center. Retrieved November 29, 2018 from http://www.pewinternet.org/2015/10/01/teens-technology-and-romantic-relationships/

[7] Anthony T. Pinter, Pamela J. Wisniewski, Heng Xu, Mary Beth Rosson, and Jack M. Caroll. 2017. Adolescent Online Safety: Moving Beyond Formative Evaluations to Designing Solutions for the Future. In *Proceedings of the 2017 Conference on Interaction Design and Children - IDC '17*, 352–357. https://doi.org/10.1145/3078072.3079722

[8] Afsaneh Razi, K. Badillo-Urquiola, and Pamela Wisniewski. 2020. Let's Talk about Sext: How Adolescents Seek Support and Advice about Their Online Sexual Experiences. https://doi.org/10.1145/3313831.3376400

[9] Pamela Wisniewski. 2018. The Privacy Paradox of Adolescent Online Safety: A Matter of Risk Prevention or Risk Resilience? *IEEE Security Privacy* 16, 2: 86–90. https://doi.org/10.1109/MSP.2018.1870874

[10] Pamela Wisniewski, Arup Kumar Ghosh, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2017. 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), 51–69. https://doi.org/10.1145/2998181.2998352

[11] Pamela Wisniewski, Heng Xu, Mary Beth Rosson, Daniel F. Perkins, and John M. Carroll. 2016. Dear Diary: Teens Reflect on Their Weekly Online Risk Experiences. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (CHI '16), 3919–3930. https://doi.org/10.1145/2858036.2858317

[12] NSF Award Search: Award#1827700 - PFI-RP: A Multi-Disciplinary Approach to Detecting Adolescent Online Risks. Retrieved December 21, 2018 from https://nsf.gov/awardsearch/showAward?AWD_ID=1827700&HistoricalAwards=false

[13] What is a Certificate of Confidentiality? | grants.nih.gov. Retrieved February 17, 2020 from https://grants.nih.gov/policy/humansubjects/coc/what-is.htm