More engagement in tech design can improve children's online privacy, security

June 22 2023, by Mary Fetzer

Credit: Unsplash/CC0 Public Domain

Children are growing up in a digital world where technology plays a role in their everyday lives. Research on human-computing interaction (HCI) shows that designing technologies for children's privacy and security

online, like parental controls and monitoring systems, and centering the interests of children in these efforts is complex and challenging.

Engaging children early and often in the development of online privacy and security features may result in technologies that better protect them while addressing their interests, according to Priya Kumar, assistant professor in the Penn State College of Information Sciences and Technology (IST), who led the multi-institution research team.

Kumar's team analyzed 90 HCI research publications from 2009 to 2019 to examine not only the problems and solutions involved with designing online technologies for children's privacy and security but also how the research engaged with children.

"We wanted to know what it means to design for children's privacy and security and find out how children were playing a role—if at all—in this work," Kumar said. "Privacy and security are complex concepts that are challenging to design for and centering the interests of children is similarly difficult."

The team found that by defining online privacy and security goals more specifically and involving children earlier in the process, technology designers may prevent conflicts between what children want and what they need to stay safe. The researchers will present their findings at the Association for Computing Machinery Interaction Design and Children (IDC) Conference, taking place June 19–23 at Northwestern University in Chicago. IDC is an international conference for researchers, educators and practitioners to share the latest research findings and new technologies in child-centered design, according to the conference website. Their findings will be published in the conference's proceedings later this year.

Using prior research to inform work on children's

privacy and security

Kumar said she believes that because the definition of privacy and security is so wide-ranging, it's important for researchers and designers working in this area to define more specifically what aspects of privacy and security they're working on and recognize that those issues may conflict with one another.

"Tension can result from designing for multiple privacy and [security issues](#)," she said. "Designers may implement parental controls or monitoring systems to keep children's data secure during digital interactions, but doing so can raise questions related to the surveillance and invasion of privacy for the children who use the technology."

Some of the reviewed research found that children express frustration with "overly restrictive and invasive" parental controls. According to Kumar, these frustrations do not mean that monitoring systems should not exist but rather that researchers and designers need to be intentional about creating systems that address the needs of the children they are intended to protect.

"Privacy and security are always going to mean lots of different things and there isn't one 'right' definition," Kumar said. "Drawing on existing theory and prior work on the topic can help researchers and designers identify their privacy and security goals and make a plan to achieve those goals."

The researchers categorized each of the papers they reviewed using a [framework developed by privacy scholar Daniel Solove](#) that identified 16 privacy and security issues across four categories: information collection, information processing, information dissemination and invasion.

Bringing children into the process of designing for privacy and security

Kumar's team focused on research involving children ages 5 to 12 and found that more than half of the papers they reviewed engaged children in some way. But they also found that the majority of those papers focused on getting feedback from children by interviewing them or showing them a prototype, tactics they said are important but involve a fairly limited amount of engagement.

"I would like to see the mentality of HCI researchers and designers shift from thinking they know what children need and want to actually centering children and their interests as much as possible," Kumar said. "We should explore how children are understanding privacy and security and how they want it to be addressed."

Additionally, she said she is hopeful that researchers and designers will notice children's privacy and security issues sooner rather than later in the course of their work.

"Ideally, they will consider—from the project's conceptualization—which aspect of privacy they're touching and bring children into their work at the earliest stage," she said. "This evolving paradigm, in tandem with the work that's already been done in this space, may contribute to the creation of guidelines and systems that truly address the privacy and security issues that children are facing in a way that the children themselves are okay with."

Kumar acknowledged that doing child-centered design—which involves time, resources, expertise and ethical insight—is more difficult than just asking children for feedback on adult-imposed visions of what we think they want. But she said she believes that good work has already been

done.

"Researchers and designers can look to the literature to see what children have said on the topic of privacy and [security](#) and build on that," she said. "They can also look to alternative ways to get children's viewpoints, such as comments and reviews on the software and apps the children are using."

Provided by Pennsylvania State University