Teacher Perspectives on Child Online Privacy and Security

Charlotte Moremen
University College Dublin

Eleanor Birrell
Pomona College

1 Introduction

In an increasingly digital society, teachers and schools today rely on technology both for logistical support and educational enhancement, and internet and computer access are also increasingly necessary for children to complete their classwork and homework, especially post-pandemic [1, 5]. This gives rise to a timely and critical question: how does the widespread adoption of technology—both socially and in educational settings—affect children's online privacy and security today?

We explore this question through the lens of a key group of stakeholders: teachers. We interviewed 24 primary and secondary school teachers who worked as full-time classroom educators at U.S. schools in the 2024-2025 academic year, expanding on prior works that focused in confined geographic areas, were conducted pre-pandemic, or interviewed other school officials [2–4].

We found that most teachers believed their students were vulnerable to significant security and privacy risks. While interpersonal privacy threats were predominant in our conversations, teachers also raised concerns about corporate privacy threats posed by both educational and social technology use. Teachers described a wide variety of security and privacy concepts and tips they taught their students, but there were no widespread patterns in exactly what was taught and most teachers confirmed that such decisions were un-standardized and entirely determined by individual educators. Additionally, our results suggest that security and privacy education is not fully integrated into the broader technology-related curriculum and that there are outstanding questions about whose responsibility it is to educate children about security and privacy.

Based on our results, we suggest potential methods of addressing these issues for educators, regulatory policy, and future security and privacy research.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2026.
August 23–26, 2026, Hannover, Germany.

2 Methodology

2.1 Participant Recruitment

All participants were pre-screened for living in the United States and working as a full-time in-classroom teacher for the 2024-2025 school year. A mixed-methods approach was utilized to recruit participants. 10 participants were recruited via community connections with the authors, and an additional 14 were recruited via Prolific to increase geographical diversity by using purposive sampling. Participants recruited via Prolific completed a brief screening survey to confirm their eligibility, for which they were paid $0.25-$0.50, depending on the length of time it took them to complete the survey. Eligible participants were then invited to sign up for a timeslot to be interviewed. Participants were recruited via Prolific until thematic saturation was reached.

2.2 Study Protocol

After consenting to participate in the study, participants completed a short demographic survey about themselves, their school, and their classroom. They were then interviewed one-on-one by the first author after reaffirming consent to having audio recorded by Zoom for transcription purposes. Teachers were asked about their students' use of technology and the internet in the classroom, for homework, and at leisure, and about what privacy and security implications they may have. They were also asked about how much influence they had on the type of technology used in their classroom, and what education, if any, is provided by the school about technology and its use. Interviews were structured via a set of pre-written questions and then an opportunity for the participant to offer

any other thoughts not yet addressed. Additionally, clarifying questions were asked about topics mentioned by participants while answering another questions.

Interviews lasted approximately 20-35 minutes, and participants were compensated with a $20 gift card or bonus payment.

2.3 Data Analysis

Data analysis was conducted using inductive coding. Both authors independently open coded all of the responses to each of the questions. We then met to discuss the set of open codes and generate a code book with standardized codes and definitions for each question. Both authors then independently re-coded all responses, tagging each response with the relevant tags from the standardized codebook. We then met again to reconcile and finalize the codings.

2.4 Ethics

To mitigate the threat of participant reidentification, no identifying information was collected from Prolific participants, and the only identifying information collected from community participants was on the consent form, which was stored securely and separately from transcripts and surveys.

Interview transcripts were stored separately from the demographic surveys and were identified only by randomly assigned participant IDs. All participants provided informed consent both to participate in the study and to have their interview recorded, and were aware that they could decline to answer a question or withdraw from the interview at any time.

This study was reviewed and approved in advance by the Pomona College Institutional Review Board.

3 Results

All of the teachers we interviewed used technology in their classroom in some ways, although the types of technology and how it was used varied. Of the themes we identified, six were directly related to online privacy and security: surveillance by parents/school, kids violating others' privacy, real world security threats, (some) kids being aware of interpersonal privacy, the data economy, and finally, questioning with whom the responsibility of child cybersecurity education lies.

School/Parental Surveillance. 14 of 24 teachers mentioned that their students' online activities are surveilled by parents or at school. Several teachers mentioned that their school had software (Hapara, Lightspeed, Gaggle, GoGuardian, and Black Sea) that allowed them to view and sometimes control student screens. Two teachers' schools had particularly advanced software that tracked certain keywords and automatically notified school administration if they were typed on a school device.

Privacy Threats from Students. 11 of 24 teachers mentioned in their interviews that students took photos or videos of other students and/or teachers and uploaded them to the Internet without their consent.

Real World Security Threats. 7 of 24 teachers mentioned real-world security threats that originated online during their interviews, primarily sex trafficking by an adult met online and school shooting threats circulating online.

(Some) Awareness of Interpersonal Privacy. 4 of 24 teachers mentioned that some of their students were aware of basic interpersonal privacy online, such as being aware of the possibility of going viral, knowing that nothing is truly anonymous, or using anonymous accounts or "finstas" (Fake Instagrams) to avoid monitoring by their parents.

Understandings of the Data Economy. 4 of 24 teachers brought up the data economy during their interview. The most common note was that students struggled to conceptualize or care about it, despite efforts such as teaching students to read through privacy notices when they pop up and requiring students to choose and read a privacy policy in its' entirety as an assignment. Two participants noted that their students enjoyed the personalization of ads, not caring or understanding that it was the result of data collection about them.

Responsibility for S&P Education. Finally, 4 of 24 teachers wondered to whom the responsibility for child cybersecurity education falls to during their interviews. One participant put it most succinctly, musing that *"in making sure that kids understand just how little information needs to be obtained by someone in order for their data and their data privacy to be at risk, the question becomes, who is the responsibility falling to?"*

4 Conclusion

After interviewing 24 K-12 teachers across the United States, we have found that teachers are concerned about a multitude of issues regarding children's online privacy and security. We strongly recommend the implementation of steps such as standardizing and funding cybersecurity education, banning data collection of users under 18, creating legal culpability for platforms for the content pushed to children on their platforms, and a reevaluation of the value of surveillance in schools. Further research should expand on this topic by critically evaluating new educational technologies for their privacy and security risks and the benefits they provide students, not the profit margins of EdTech companies.

References

[1] S. Babić, S. Križan Sučić, and G. Sinković. Understanding the factors that influence secondary school teachers' intention to use e-learning technologies for teaching after the covid-19 pandemic. *2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO)*, pages 848–853, 2020.

[2] Jake Chanenson, Jason Chee, Navaneeth Rajan, Danny Huang, Marshini Chetty, Brandon Sloane, and Amy Morrill. Uncovering privacy and security challenges in k-12 schools. *CHI '23: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, (Article 592):1–28, 2023.

[3] Adolph Delgado, Liane Wardlow, Kimberly O'Malley, and Katherine McKnight. Educational technology: A review of the integration, resources, and effectiveness of technology in k-12 classrooms. *Journal of Information Technology Education: Research*, 14:397–416, 2015.

[4] Priya C. Kumar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. Privacy and security considerations for digital technology use in elementary schools. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, (Paper 307):1–13, May 2019.

[5] Zhuojing Zhang and Sarrah Wasie. Educational technology in the post-pandemic era: Current progress, potential, and challenges. In *Proceedings of the 15th International Conference on Education Technology and Computers*, pages 40–46, 2023.