Privacy and Security Considerations For Digital Technology Use in Elementary Schools

Priya C. Kumar
College of Information Studies
University of Maryland
College Park, Maryland
pkumar12@umd.edu

Marshini Chetty
Department of Computer Science
Princeton University
Princeton, New Jersey
marshini@princeton.edu

Tamara L. Clegg
College of Information Studies
University of Maryland
College Park, Maryland
tclegg@umd.edu

Jessica Vitak
College of Information Studies
University of Maryland
College Park, Maryland
jvitak@umd.edu

ABSTRACT

Elementary school educators increasingly use digital technologies to teach students, manage classrooms, and complete everyday tasks. Prior work has considered the educational and pedagogical implications of technology use, but little research has examined how educators consider privacy and security in relation to classroom technology use. To better understand what privacy and security mean to elementary school educators, we conducted nine focus groups with 25 educators across three metropolitan regions in the northeast U.S. Our findings suggest that technology use is an integral part of elementary school classrooms, that educators consider digital privacy and security through the lens of curricular and classroom management goals, and that lessons to teach children about digital privacy and security are rare. Using Bronfenbrenner's ecological systems theory, we identify design opportunities to help educators integrate privacy and security into decisions about digital technology use and to help children learn about digital privacy and security.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**; • **Social and professional topics → Children**.

KEYWORDS

privacy, security, technology use, elementary school

CHI 2019, May 4–9, 2019, Glasgow, Scotland UK

ACM ISBN 978-1-4503-5970-2/19/05…$15.00
https://doi.org/10.1145/3290605.3300537

ACM Reference Format:
Priya C. Kumar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2019. Privacy and Security Considerations For Digital Technology Use in Elementary Schools. In *CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019, Glasgow, Scotland UK*. ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3290605.3300537

1 INTRODUCTION

Schools across the United States have integrated Google, Microsoft, and Apple products into K-12 classrooms [44]. However, the widespread use of these technologies—sometimes with little to no training for the educators using them—raises privacy and security concerns. These concerns include how schools monitor students' technology use [21], what data corporations get when students use their devices [44], and how schools use the student data they collect [15]. Much existing work by researchers, journalists, policy makers, and activists focuses on student data privacy issues. For instance, nearly 350 organizations have signed a "Student Privacy Pledge" committing to principles of responsible data management [2]. However, less attention focuses on how individual educators consider privacy and security when using technology in their classrooms and what educators teach students about digital privacy and security [18].

Our paper addresses this gap. Doing so is important because elementary school students regularly use digital technology for educational purposes, making schools a logical place for them to learn how to navigate privacy and security online [11]. Educators also play an important role in determining how technologies can be used to enhance learning [34]. Understanding how educators navigate digital privacy and security issues—as well as how they teach children about these concepts—is crucial for finding design opportunities to teach children about privacy and security online. To do this, we ask three research questions:

(1) What digital technologies do elementary school educators use in the classroom?

(2) How do considerations about privacy and security inform digital technology use in elementary school classrooms?
(3) What digital privacy and security lessons do elementary school educators give students?

We conducted nine focus groups with 25 educators from three metropolitan areas in the northeast U.S. Our findings reveal that digital technologies are an integral part of elementary school classrooms, and educators primarily consider privacy and security as it relates to handling student data and minimizing inappropriate use of technology. They rarely teach children lessons specifically about privacy and security, with some feeling that such lessons are unnecessary for younger children. Others saw privacy and security as part of topics like digital citizenship and suggested ways to make such lessons resonate with children.

We interpret these findings through the lens of Bronfenbrenner's ecological systems theory [7, 8]. Various contexts shape children's experiences, including the classroom, home, and society at large. Our study focuses primarily on the microsystem of the classroom, but our findings highlight design opportunities across contexts that can help children learn about digital privacy and security.

2 RELATED WORK

To situate our study, we review existing work on privacy and children's digital technology use, the role teachers play in integrating technology in the classroom, and how an ecological approach can help us understand digital privacy and security in the school context.

Children, Technology Use, and Privacy Education

From tablets to connected toys and netbooks to course management software, digital technology is deeply embedded into children's everyday experiences at home [32] and school [30]. Privacy implications related to digital technology use range from abstract concerns about surveillance and identity theft to everyday tensions such as "minimizing embarrassment, protecting turf (territoriality), and staying in control of one's time" [37, p. 130]. Identity theft may not be a top concern for elementary school children (though it can happen [13]), but this does not mean that privacy is irrelevant to children's technology use. To the contrary, privacy enables children to feel comfortable when communicating with peers, forming relationships, seeking advice, and engaging in identity play [27, 50]. Nevertheless, children may not always make connections between online and offline privacy [35].

HCI researchers are actively exploring children's perspectives on—and knowledge of—privacy and data sharing in online spaces. One study found that children ages 8-16 who used the visual programming language Scratch discerned some of the privacy implications of making data publicly available and searchable [19]. For example, they understood that data collection and retention implicate privacy, that data analysis requires skepticism and interpretation, and that data includes assumptions and hidden decision-making. Another study found children ages 6-10 knew that Internet-connected toys could "remember" what children said via recordings, but they did not make the link that others could also hear the recordings [33]. Likewise, we conducted a study with children ages 5-11 and found they had a basic understanding that information could be sensitive and should be shared only with trusted parties; however, these children had little understanding of more complex topics such as how the medium of communication (e.g., face-to-face vs. online) implicates privacy [24]. Overall, these studies suggest that while children absorb aspects of how privacy plays out online, they may need support understanding more nuanced ideas.

Parents are an obvious source of support to help children develop privacy and security skills. However, in our study with elementary school-aged children, we found some parents saw privacy and security as a future concern, rather than something for their children to understand now [24]. Some parents may also have a limited understanding of privacy and security. The Pew Research Center found the typical American adult Internet user can only answer five out of 13 basic cybersecurity questions correctly [45]. Factors including age, education, socioeconomic status, and profession influence people's cybersecurity skills [40]. Thus, while parents are a natural source of information for children, they should not—and perhaps cannot—be the only source.

Schools can also play an important role in helping children develop privacy and security skills [11], especially as educators continue to integrate digital technology into their curricula. Some resources exist to teach privacy and security in high school [3], middle school [14], and elementary school [17]. That said, American children do not generally receive formal lessons about digital privacy and security [20]. In addition, larger questions remain about the privacy implications of digital technology in the classroom in the first place. For example, Internet access in classrooms enables schools and corporations to surveil students, characterizing school as not just a source of learning but also a place to regulate and control children's behavior [49]. Thus, while school may be a place for children to learn about privacy, technology use in school can also pose challenges to students' privacy.

Educators' Role in Integrating Technology in Schools

Research on technology integration in schools has largely focused on educators' use of technology to transform pedagogy [5, 22, 23], since educators guide and plan the use of technologies in their classrooms [46–48]. The creation of resources for educators (e.g., professional development,

technical support) can help teachers transform learning and teaching experiences instead of enacting the same learning activities using technology [5].

To advocate for the integration of technology into every part of teaching, Mishra and Koehler [34] developed the Technological Pedagogical Content Knowledge (TPCK) framework. They specify that teachers not only need knowledge of specific tools, hardware, and software that can be used for learning (Technology Knowledge), but also that this knowledge needs to be deeply integrated into their understanding of how people learn (Pedagogical Knowledge) and their knowledge of the discipline in which they teach (Content Knowledge). Though a large body of research has focused on technology use in schools as well as educators' TPCK (e.g.,[16, 22, 23, 36, 42], we could not find any studies that considered the intersection of TPCK and digital privacy and security in elementary schools.

Our research contributes to this literature by examining how educators use digital technologies in elementary school classrooms, how privacy and security factor into this use, and what students learn about digital privacy and security.

An Ecological Systems Approach to Understanding Privacy & Security in Schools

To gain a holistic perspective on how educators can help students learn about digital privacy and security, we consider our findings through the lens of Bronfenbrenner's ecological framework [7, 8]. This framework emphasizes the need to understand students' experiences in situ, taking into account multiple layers of context that influence one's experience. This means considering learning as it occurs in microsystems, mesosystems, exosystems, macrosystems, and chronosystems. Figure 1 shows how we apply this framework to the elementary school context.

Microsystems involve direct interactions with students; they are places where students engage in specific activities and take on roles for particular periods of time (e.g., classroom settings where teachers directly interact with students). The mesosystem describes the interrelationships among major settings of a student's life (e.g., school, neighborhood, and community settings). The exosystem represents the social structures that influence the immediate settings in which students interact (e.g., school or district policies). The macrosystem denotes the overarching institutions of culture or subcultures that encompass micro, meso, and exosystems (e.g., laws and societal trends). Finally, the chronosystem refers to change over time in individuals, environments, and the relations between them.

With this framework in mind, education researchers recognize that a range of contextual factors influence technology use in schools as well as educators' use of transformative pedagogies with technology [42]. For example, decisions made at school and district levels determine what technologies are available in classrooms, what policies govern technology use in schools, and what, if any, professional development or support educators receive [51]. Other settings in which children use technology (e.g., home, community) and broader societal factors (e.g., technology trends) also affect technology use (and non-use) in the classroom [42].

Though the TPCK framework emphasizes the complex role that micro, meso, and macrosystem contexts play in professional development and innovations in learning and teaching with technology, most studies of TPCK have not addressed context [42]. These studies have typically focused on learning outcomes for students or professional development outcomes for educators. In addition, the role of context as it relates to technology use and digital privacy and security learning is understudied.

In the HCI community, education-focused research has begun exploring technology use in schools at these contextual levels. Most research focuses on the microsystem, emphasizing the influence of specific technologies or pedagogical approaches used in a particular classroom on learning (e.g., [10, 28–30]). At the meso, exo, and macrosystem levels, education research has considered the influence of school, district, and federal policies and procedures on the use of technologies in schools (e.g., [46, 47, 52]). However, with the exception of Ahn et al. [4], who studied the use of social media and tangible displays across school, home, and community settings (i.e., mesosystem level) and Pittarello et al. [38], who hosted a workshop at CHI-Italy 2017 to explore HCI in various educational settings (i.e., macrosystem level), little HCI research has focused on the meso or macrosystem levels of technology use in schools.

Although our study primarily focuses on digital privacy and security in the microsystem of the classroom, participants also discussed meso and exosystem influences, such as parents and school district leaders. Based on our findings, we provide design recommendations for each level of Bronfenbrenner's framework [7, 8].

3 METHODS

To understand how privacy and security factors into digital technology use in elementary school classrooms, we conducted nine focus groups with 25 educators (M=33 years old, SD=11, range: 22-64) from seven school districts in three metropolitan regions in the northeast United States between August 2017 and February 2018. Our participants included teachers, teaching assistants, student teachers, and graduate students who taught as part of their program. All but two worked in elementary school classrooms. To gauge our participants' privacy and security awareness, we asked them to fill out the privacy-related attitudes and behaviors scale [9]

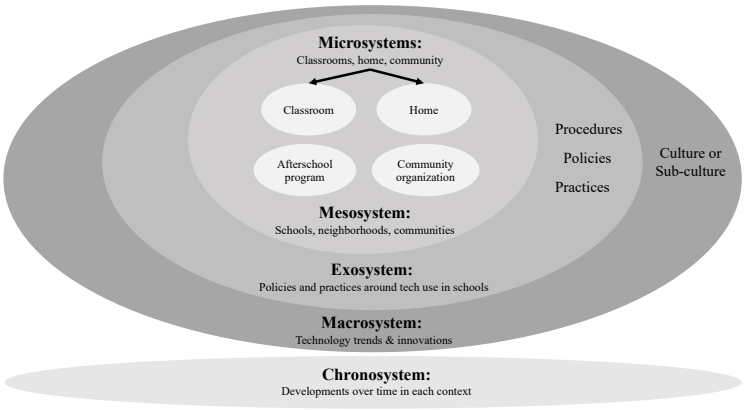

Figure 1: Bronfenbrenner's ecological framework applied to the school context.

(M=3.2, SD=0.8) and Security Behavior Intentions Scale (SeBIS) [12] (M=3.3, SD=0.6). Overall, the 22 participants who filled them out were slightly above average when it came to privacy and security concerns and behaviors. Eight participants also reported receiving some technology training focused on privacy and security. Table 1 shows participant demographic information.

To recruit participants, we posted on educator-focused listservs and groups on Meetup and Facebook as well as asked educators from our personal networks to share study information with people they knew. We also partnered with a teacher certification program at a university and conducted two focus groups in one of the program's courses. Each participant received a US$15 Amazon gift card. The University of Maryland's Institutional Review Board (IRB) approved this study.

Data Analysis

After the focus groups were transcribed, the research team collaboratively developed a codebook and went through multiple rounds of structural coding and thematic analysis [43]. To create the codebook, each author reviewed a different transcript and the team discussed the relevant categories that emerged. We created codes for the technology educators used, decisions about technology use, rules or boundaries around technology use, technology-related challenges, parent-teacher communication, privacy/security lessons, and technology-related training for educators. We then went through two rounds of structural coding [43] in which one researcher applied the codebook to the transcripts and another researcher reviewed the transcripts and refined the coding. The team then conducted a thematic analysis on the coded data [43]. Each author selected two to three codes, reviewed the quotes in each code, clustered similar quotes, and summarized them in thematic statements. The team met repeatedly throughout the coding to discuss these ideas, reach consensus on the main themes in the data, and distill them into findings.

By nature, focus groups allow participants to guide the conversation and build on the experiences of others. Consequently, some focus groups discussed certain topics and/or experiences in greater depth than others. When reporting our findings, we refrain from using quantitative metrics of how many participants made a given statement because the themes discussed here emerged from more general questions or prompts rather than a narrow accounting where we sought feedback from each participant. Qualitative theorists have provided several arguments against reporting qualitative data numerically, one being that, "[n]umbers can lead to the inference (by either the researcher or the audience) of greater generality for the conclusions than is justified, by slighting the specific context within which this conclusion is drawn" [31, p. 479]. For this reason, we focus our findings on the themes that emerged across the full dataset rather than a numerical accounting of who said what.

4 FINDINGS

To address our research questions, we summarize the types of digital technologies educators use in their classrooms, explain how digital privacy and security factors into this technology use, and describe how educators teach students about digital privacy and security.

Digital Technology Is Omnipresent in Elementary School Classrooms

Participants described using a variety of technologies in the classroom. Some of their school districts offered one-to-one device programs where each student in a grade received

Table 1: Focus Group Participant Information

Focus Group	Participant	Role in School	Type of School
1	Alison	Teacher: Grade 5	Public elementary
1	Bernard	Former substitute teacher	Public elementary
2	Cindy	Teacher; Grade 1	Public elementary
2	Diane	Teacher: Grades 4-6	Private Montessori
3	Emilia	Teacher: Kindergarten	Public elementary
3	Norah	Teacher: English as a Second Language (ESL)	Public elementary
3	Gabriela	Teacher: Science resource	Public elementary
3	Hannah	Teacher: Arts and humanities	Public elementary
4	Irene	Teacher: Special education	Public elementary
4	Jasmyn	Teacher: Grade 3	Public elementary
5	Marisol	Teacher: Pre-K (age 4)	Public charter elementary
5	Luz	Teacher: Pre-K (age 4)	Public charter elementary
5	Maryam	Teacher: Pre-K (age 4)	Public charter elementary
5	Ayana	Assistant teacher: Pre-K (age 3)	Public charter elementary
6	Inez	Taught a 7th grade class as a graduate student	Middle
7	Paul	Taught a 6th grade class as a graduate student	Middle
7	Ridhi	Taught a 4th grade class as a graduate student	Elementary
8	Stephanie	Student teacher: Grade 5	Public elementary
8	Tess	Student teacher: Grade 1	Public elementary
8	Victor	Student teacher: Grade 4	Public elementary
8	Yvonne	Student teacher: Grade 5	Public elementary
9	Alissa	Student teacher: Grade 5	Public elementary
9	Bethany	Student teacher: Grade 5	Public elementary
9	Caitlyn	Student teacher: Grade 1	Public elementary
9	Dawn	Student teacher: Grade 2	Public elementary

their own device for educational activities. In others, educators and students had access to shared computers, laptops, or tablets as well as interactive smartboards, document cameras, and/or projectors. Educators mentioned using productivity software (e.g., Google Apps), learning management systems (e.g., Canvas, GoGuardian, Hapara), presentation tools (e.g., Screencastify, LiveBinder), media platforms (e.g., YouTube), media editing software (e.g., iMovie, Powtoons), interactive quiz tools (e.g., Kahoot, Quizlet), communication apps (e.g., ClassDojo, Remind), educational databases (e.g., BrainPOP, PebbleGo), math and reading websites or apps (e.g, iReady-Math, Starfall), and games (e.g., ABCya!). They also looked for technology-related resources for their students on sites such as International Society for Technology in Education (ISTE), CommonSense Media, and Teachers Pay Teachers.

Participants said their students used digital tools to look up information, to complete assignments or projects (e.g., write stories or essays, create presentations), to more easily interact with information (e.g., listen to a story rather than read it), and to take standardized tests. Educators told us they also used these technologies in varied ways: to display information during class time, to make lessons interactive, to share materials for students to make up or practice lessons at home, to develop lesson plans, to record data about students and monitor their educational progress, and to communicate with students and parents.

Educators said they looked for tools that focused on the content their students were learning (e.g., math, science, reading) and aligned with students' developmental abilities (e.g., pictures and simple words for students who were learning to read). They tried to avoid tools that involved a lot of typing or complex login processes, since these were challenging for students, especially younger ones, to use. Beyond supporting students' learning, educators also reported using technologies to facilitate time-consuming tasks (e.g., grading) and to

help manage their classrooms (e.g., monitoring student technology use to deter students from engaging in inappropriate activities).

Educators Consider Privacy and Security Through the Lens of Curricular or Classroom Management Goals

Considerations about digital privacy and security emerged in three aspects of classroom technology use: deciding what technologies to use, handling student data responsibly, and minimizing students' inappropriate use of technology. Our participants were largely focused on how these decisions would affect their ability to teach students what their curricula required and to manage student behavior.

Deciding Which Technologies to Use in the Classroom. Participants typically used digital tools that were available or recommended to them. They described turning to school media specialists for help deciding what to use in the classroom. Media specialists might suggest relevant tools for a specific assignment or identify resources that fit with the district's curriculum and learning objectives. Some districts provided lists of applications or websites for which they had purchased software licenses and/or approved for classroom use. Third-grade teacher Jasmyn explained that if apps appeared in this list, it meant:

> "They're all free, and they're all education-based apps. Something that [the district has] looked at and said, 'This is okay to put your students onto.' So it kind of narrows down your search if you're looking for something." (Jasmyn)

Educators said they did not know how their school districts decided to purchase particular hardware (e.g., Chromebooks, iPads) or software (e.g., Google Apps for Education). Some technology decisions seemed to be responses to concerns that emerged from earlier decisions. For example, fifth-grade teacher Alison explained that a few years after her district gave students Chromebooks, it purchased the "Chromebook management tool" GoGuardian:

> "It allows the teacher to log in and see everybody's Chromebook, and you can close out tabs if students are on the wrong thing.... We just got that the end of last year... because there were so many issues with kids doing things on Chromebooks, so they finally figured it out, that we needed this." (Alison)

Other software-related decisions happened at the school level. For example, Alison said her district created a learning management portal but let each principal decide whether to use it in their school.

Overall, participants did not know whether school districts or media specialists considered how a tool used students' personal information before recommending it. Some educators expressed concern about using software that required too much student information, such as names, email addresses, or birth dates. A few used limited identifiers, such children's initials. One avoided using any tools that required more than an email address to sign up.

Participants said they received some training related to the various technologies their schools had adopted, but this typically did not include information related to privacy and security. Some training only focused on basic activities, such as how to post grades, or was only available to a few teachers from each school. Few educators described training experiences directly related to privacy or security. For example, Jasmyn paid for a professional development class through her district's technology development office. One of the steps in an app review she conducted for the class was to check the app's privacy policy— "*which now in turn, has made me just peek through privacy policies*" when she considers using an app in her classroom. While privacy and security played some part in the decisions educators made about technology use in the classroom, it was unclear whether such considerations were institutionalized at the school or district level.

Handling Student Data Responsibly. Participants recognized their duty to responsibly manage student data, which primarily included login credentials and photographs of children engaging in school activities. Again, policies or priorities at the school or district level complicated educators' efforts to mitigate privacy or security concerns.

Policies for creating student accounts varied considerably. In some districts, student passwords used the child's name, birth date, and/or ID number; in others, passwords could not contain any part of a student's name. One participant said she manually reset student passwords for her school each year while another said students in her district keep the same password throughout elementary school. Educators said they had to help students manage their credentials:

> "One of the things they found in first grade, they gave all the kids computers and realized the kids don't know their upper- and lowercase letters. So, they can't put in their passwords.... Teachers are doing it for them because they don't know their letters." (Norah)

Other ways to help students remember login credentials included sending the credentials home to parents or keeping them in a box that they passed around when students had to log in. Two participants described cases of student passwords being taped to equipment.

Participants also discussed their thought processes related to posting student photos on school or district websites,

newsletters, and social media. This involved balancing the school or district's desire to publicize educational activities with parental permission to share images of children. For example, Hannah, an art teacher, liked the idea of sharing her students' work on social media but called it a "*double-edged sword*" because some parents may have opted out of having their child's picture taken during the school day or at school functions. This opt-out could mean that students would not appear in the yearbook or could miss out on field trips where pictures would be taken. Norah, an English-as-a-Second Language (ESL) teacher, noticed that most of her students were on her school's opt-out list. She surmised their parents may have signed it without understanding it.

Overall, the educators in our focus groups understood the need to manage student data responsibly, but school policies sometimes challenged their ability to do so.

Minimizing Inappropriate Use of Technology. Educators expressed wanting their students to learn how to use technologies responsibly and to minimize students' inappropriate use of technology. Two participants created classroom contracts related to technology use. Others said they discuss physical use of devices (e.g., don't run with them), how to navigate concerning scenarios, (e.g., seeing something inappropriate), and how other classroom norms apply to technology use (e.g., respecting materials, sharing with others).

Participants also wanted to manage how their students were using digital technologies. First, they wanted students to use the devices only at designated times and to go to specific websites or applications that teachers had assigned to them. Second, they wanted students to avoid accidentally or intentionally accessing adult information, such as sexually suggestive or drug-related material. Third, they wanted to reduce student exposure to advertising because this material could distract students during lessons or present inappropriate material.

Some educators described walking around or relying on the classroom layout (e.g., computers arranged in a semi-circle) to observe whether students were on task. Others used tools like Google Classroom or LiveBinder to list the websites or apps that students were supposed to access for a given assignment. Alison said that while her students were working on a project, she displayed all students' Chromebook screens on the projector. This way, everyone would see if one veered off-track. Two participants described learning management software that tracked students' activities as "*useful*." By enabling educators to see and take screenshots of students' screens, in the present moment or in the past, the software produced "*evidence*" they could send to parents or school administrators if an issue arose. Educators said that students who accessed inappropriate material online or went to sites without permission faced consequences such as removal of computer privileges or automatic referrals to the school's office or behavioral support team.

The educators we spoke to wanted to minimize the chance of encountering adult material during lessons. For example, Tess said searching for information "*backfired*" in her first-grade classroom when, during a lesson on storytelling, someone searched for "climax" and "*other things came up.*" Participants said they avoided searching for information on search engines or platforms like YouTube while projecting their screen to the class, since they did not know what would appear in response to the search. Others said they turned off projectors while searching for information, used tools such as Safeshare.tv, which displays videos without advertising or recommendations, or avoided using tools that contained pop-up advertising.

In sum, educators' efforts to reduce inappropriate use of technology focused on protecting students from online risks and monitoring their use of technology.

Lessons About Privacy and Security Online Are Rare

Few participants described giving their students specific lessons related to privacy and security; some felt such lessons were unnecessary for young students. Participants expressed varied interpretations of the role of privacy and security in students' lives, connecting it to digital citizenship and the disclosure of personal information. They offered ideas about how such lessons could be designed to resonate with elementary school students and identified obstacles educators face in teaching students about privacy and security online.

The Role of Digital Privacy and Security in Students' Lives. Our participants conceptualized privacy and security for students as a subset of digital citizenship, which they defined as learning how to act responsibly online. For instance, Jasmyn described the connection between digital citizenship and privacy as, "*What are you doing online? How will you be leaving a digital footprint?*"

Only a few educators said their students received lessons focused on digital privacy and security, and these typically came from a school media specialist or librarian. For instance, Hannah said her school's media specialist dedicated a session for each class in the school to "*talking about [students'] technology footprint.*" She added that the media specialist wanted to discuss cyberbullying in a digital citizenship lesson after students at the school experienced bullying through Snapchat. In a similar vein, two student-teachers said their fifth-grade classes received a lesson at the media center about "*how to be safe online and what kind of technology is appropriate for their age and, kind of, how it can affect their getting into college, getting a job.*" (Stephanie)

Conversely, Diane described how her school incorporated discussions about digital privacy and security in an unexpected context—sex education:

> "One of the weeks is dedicated to technology use and how to be safe, because so much of… our sex ed is actually about communication: how to communicate with one another and how to communicate respectfully. And the same thing goes for technology. We do talk about privacy and talk about responsible technology use and about miscommunications that can happen over technology." (Diane)

Some participants said discussions about privacy and security were less necessary because elementary school students only used technology in limited ways. For example, Ayana, a pre-K teacher, said her three-year-old students could not access much on the iPads they used. Jasmyn said she did not discuss privacy and security in-depth with her third graders because "*they're not on chat rooms and Facebook.… I'm sure [for] the secondary [school] teachers, that's another debate for them.*" Similarly, Alison felt privacy and security lessons were not necessary for her fifth graders because they did not enter personal information when using digital technology:

> "They're using the Chromebooks kind of on the most basic level, where they're using word processors to write. And they're using Google to search on specific websites that we give them. They're never putting their own information in. Any account that they get is already set up for them. So they just have to log in with what we give them. So, there's not really much teaching on how to be safe on the Internet, knowing how to put in personal information, things like that, because it doesn't apply.… So, there's no kind of context to teach it in." (Alison)

Making Privacy and Security Lessons Resonate with Younger Children. Although privacy and security lessons were not prevalent in their teaching, participants shared ideas to make such lessons stick. Echoing prior work [25], they emphasized the need for privacy and security lessons to be relatable.

Paul, who taught a sixth-grade class about privacy and security while he was a graduate student, said he found structuring lessons as conversations rather than didactic lectures helpful. He also tied examples back to the tools his students used. For example, his students did not use Facebook, so he discussed Snapchat and Kik, which they did use. Inez, who taught privacy and security lessons to a seventh-grade class while she was a graduate student, suggested starting with examples of privacy or security based in the physical world ("*Do they have their own room? Do they close the door to their room? Do they go to the bathroom with the door open? Why do you close the door to go to the bathroom?*") and using those to help children see how privacy and security play out online. Dawn, a student-teacher, suggested giving children concrete examples, such as showing them how a piece of information can spread online or how visible a social media profile can be. She compared this to models that show young children how germs travel:

> "Where someone coughs on their hand and shakes someone's hand, opens the door and all of the germs that get left behind, I think that that's something that [students] can be like, oh, ugh, and make that connection." (Dawn)

Alison felt the experience of making mistakes helped her fifth graders understand the consequences of sharing access to information. For peer editing exercises, she encouraged students to swap Chromebooks rather than give each other electronic access to a Google Doc. Sometimes, when students did the latter and a student (accidentally or purposefully) deleted another student's work, she would let students "*sweat a little bit*" before restoring the document. She told them:

> "'Well, this what happens when you share it with someone. You don't know what they're going to do it.…' But you have to use that as a moment to be like, 'Hey, don't. You can't trust that person. You thought you could but apparently you couldn't.'… So, that's, I feel, like the biggest lesson in privacy that they get." (Alison)

Obstacles to Teaching Digital Privacy and Security Lessons. Participants also discussed various obstacles that hinder efforts to teach students about privacy and security. First, students might struggle to consider the long-term implications or consequences of disclosing information online. Paul said his sixth graders did not always absorb privacy and security lessons because they struggled to envision longer term consequences of their online actions:

> "They were definitely receptive to the idea [that technology use might affect college applications, job applications, or relationships] and a lot of them knew that it was an issue …. But it was something that was far off for them, and so it was hard for them to, oftentimes, map that onto the decision-making that they were entering into on a day-to-day basis right now." (Paul)

Second, educators may struggle to incorporate privacy and security lessons amidst other competing demands. Gabriela, who served as her school's media specialist for three years, saw this as part of her job but said she lacked the time to do so thoroughly:

> "I know as the library and media specialist, it's kind of my duty to do it.... I have not unfortunately gotten to it as much as I would like to. But I do try to instill on them, like you're saying, if you post it [online], it's there. Even if you try to delete it, it's there. It's never gonna go away, so just be careful what you put on the Internet.... But I need to do more extensive security and privacy stuff. (Gabriela)"

Finally, educators saw the need to involve parents in teaching students about privacy and security online. Some school districts offered workshops or other programs to inform parents about what technologies were used in the classroom. But participants recognized they could not take parental digital literacy for granted.

> "It would be more effective in getting the kids to understand these topics if the parents understand it, too. Because a lot of times I feel like adults don't really get it much, unless you're in a very specified area. Day-to-day, regular adults, they just don't get it. If the regular adults don't get it, you can't expect the kids to get it, if it's not especially going on constantly." (Inez)

Some participants said they encouraged their students to "teach" the digital citizenship lessons they learn in school to family members.

5 DISCUSSION

Our findings suggest that technologies are an integral part of today's elementary school classrooms. The educators we spoke to primarily consider digital privacy and security as it relates to handling student data and minimizing inappropriate technology use. They saw privacy as a subset of digital citizenship but said that students rarely received lessons directly focused on privacy or security. In this section, we identify opportunities to integrate lessons about privacy and security for elementary school children at each level of Bronfenbrenner's framework [7, 8].

Microsystem: Integrating Privacy and Security Features and Lessons into Classroom Technology

The educators we spoke to primarily consider digital privacy and security through the lens of curricular or classroom management goals. We see opportunities for the HCI community to design technology that meets educators' privacy and security needs and highlight teachable moments related to privacy and security.

Incorporate Privacy and Security Features that Meet Educators' Needs. Our participants struggled to manage student account credentials, and the policies they said their districts followed did not generally align with tenets of strong password management. Designers should consider using alternative password schemes for younger users. For instance, Assal et al. [6] found evidence that graphical password authentication might work better for children than more traditional, text-based approaches. Our findings suggest that when creating such features, designers must remain mindful of children's varied abilities (e.g., reading, fine motor skills), even among children of the same age.

Our participants also discussed privacy concerns related to posting images of students in school publications or official social media channels. HCI researchers could develop interfaces that help educators better manage sharing information while maintaining student privacy. For example, Li et al. [26] designed several approaches to obfuscating pictures so that individuals cannot be easily identified. Our findings suggest that educators may welcome such features in social media platforms, apps, and other educational technologies that involve photos in school settings. Further research towards this end is needed.

Design Technology that Highlights Teachable Moments Related to Privacy and Security. Few educators we spoke to teach their students about digital privacy and security. Echoing prior work on parents' perspectives of privacy and security for children [24], some educators we spoke to did not see such lessons as necessary for elementary school students. They perceived that these students' technology use is constrained and that these students have difficulty understanding the long-term implications of their online behaviors.

One way to help students and educators consider privacy and security early on is to design teachable moments within technologies. Read and Cassidy [39] suggest that password interfaces for children should display various warnings when the password is weak; we suggest framing such prompts in an educational rather than punitive manner. For example, a prompt could ask the user why a particular password is weak or how it can be improved. Similar to Wang et al.'s work on Facebook privacy nudges [53], educational technology interfaces can suggest that students think twice before entering personal information or can explain where data goes after they hit "Submit." Such prompts could offer a lightweight way to encourage students to think about privacy and security and also remind educators how these topics apply to elementary school students.

Mesosystem: Incorporating Digital Privacy and Security Lessons Across School and Home Contexts

Our participants recognized school as a place for students to learn about privacy and security, even if some felt such lessons were more necessary for older students. They also highlighted the important role parents play in providing and

reinforcing lessons about privacy and security online. Yet parents may also feel that such lessons are more important for older children [24] or may not fully grasp digital privacy and security issues themselves. To bridge this gap, We suggest ways to design apps that facilitate communication between educators, parents, and students.

Connect Teachable Moments Across School and Home Contexts. Our participants mentioned using mobile apps like Class Dojo and Remind to communicate with parents. Both apps offer various privacy resources on their websites, including a list of frequently asked questions for parents and details about their privacy and security protections.[1] Designers can consider embedding messages or prompts that highlight these measures within the app and suggest ways for educators and parents to discuss them with children.

For example, both apps tout their compliance with various privacy laws, including the U.S. Children's Online Privacy Protection Act (COPPA), the U.S. Family Education Rights and Privacy Act (FERPA), and the European Union's General Data Protection Regulation (GDPR). A prompt in the app could highlight these certifications and offer conversation starters to help educators or parents talk to children about why such laws matter (e.g. How do you feel about someone being able to go to school and look up your grades? Why do you think there are laws against that?). The goal is not to encourage adults to explain the nuance of privacy laws to children,[2] but rather to prompt conversations between children and the trusted adults in their lives about the value of privacy and security. Such apps could also be designed to allow educators to create prompts or messages to encourage parents to discuss the topics with children at home, helping to reinforce lessons across the school and home contexts. Future work could investigate other ways to integrate conversation starters for parents into tools designed to facilitate home-school communication.

Exosystem: Improving Educators' Knowledge about Digital Privacy and Security

Our findings suggest that decisions made at the district or school leadership level shape what technology is available or prioritized for use in the micro system of a classroom or the mesosystem of classrooms and homes. The educators we spoke to said they did not know whether or to what extent school leaders considered digital privacy and security in these decisions. But it was clear that these decisions influence everything from login and password policies to what sites students can access to what student data can be shared publicly. Beyond clarifying their own decision making processes to educators, school leaders can also equip educators to consider privacy and security in their decision-making.

Develop and Disseminate Resources that Help Educators Understand and Evaluate Digital Privacy and Security Concerns. We encourage school districts to provide educators with resources to help them vet technologies. For example, CommonSense Media maintains a database of educational technology reviews and ratings [1]. These resources should clearly explain what criteria are used to evaluate the technologies, and these criteria should take into account privacy and security. For example, these lists could explain what data the technologies collect, how they use it, how long they retain it, what happens to this data if the tool is discontinued, and whether they comply with laws like COPPA [41]. They should also explain why these criteria are important and how they affect students. This would not only help educators incorporate privacy and security into their decision-making, but also better understand how technology use can affect their students' privacy and security.

Incorporate Privacy and Security into Efforts to Build Technological Content Pedagogical Knowledge (TCPK). Our findings point to the need to consider privacy and security as a core component of educators' TCPK [34, 42]. Even though all the educators we spoke to used digital technology in the classroom, only one-third said they received any technology training related to privacy and security. Some encountered it through coursework in educational technology, while others sought relevant professional development through their districts. Our work suggests that school districts and teacher education programs should incorporate privacy and security into any existing technology training they provide to educators. Technology designers should also incorporate privacy and security into any training or onboarding materials they produce for educators.

Macrosystem and Chronosystem: Addressing Tensions Related to the Datafication of Education

Since computers and the Internet began entering classrooms more than two decades ago, scholars and journalists have considered the privacy implications of educational technologies [15, 44, 49]. Our findings suggest that educators rely on others, from school district leaders to media specialists, to vet digital technologies for privacy and security concerns. While future work should study whether and to what extent this is the case, we argue that those who develop education technologies should design them in ways that respect privacy and ensure security. In addition, the technologies should be designed so that users clearly see and understand why these

[1] See https://www.classdojo.com/privacycenter/ and https://www.remind.com/trust-safety

[2] Which probably interests zero children and few adults.

privacy and security measures are important. Making privacy and security elements more visible within technologies can help build educators' TCPK and students' knowledge.

Meaningfully doing so would require the HCI and other communities to grapple with various tensions that emerge from the datafication of education. For example, some see collecting and analyzing data as the key to improving children's educational outcomes, while others question the effectiveness of such measures [15]. Companies like Google, whose educational platform dominates American classrooms, including those of our participants, offer technologies that facilitate classroom activities, but they also profit from tracking users [44].

Finally, our findings suggest that students interact with digital technologies as early pre-kindergarten. Those who design educational technologies should consider how their technologies may be used as children grow. For example, if a math app is primarily for first graders, will its data automatically be deleted when users move to second grade? Those who create materials to teach students about privacy should do so with an eye toward what will resonate with children now but also prepare them for privacy challenges they may face in the future. For example, privacy materials for young children can use physical-world examples as metaphors for digital privacy (e.g., equating logging out of a website with closing a door).

Limitations and Future Work

While we spoke with a variety of educators, they primarily worked in public schools in metropolitan areas. Future work should consider the perspectives of educators in rural or low-income areas, as well as those who work in other types of school environments, such as private or home schooling. Future work should also take an in-depth look at other levels of Bronfenbrenner's framework. Studies of the mesosystem can examine how to incorporate privacy and security lessons across home and school contexts. Studies of the exosystem can explore whether and to what extent district leaders consider privacy and security when making technology-related decisions. As public consciousness about privacy and security issues related to digital technologies rises, studies of the mesosystem can critically question the role of technology platforms in education (something our team is currently exploring). Finally, longitudinal studies related to privacy and security learning could yield insights regarding the chronosystem.

6 CONCLUSION

Our study revealed that educators primarily consider digital privacy and security within broader curricular and classroom management goals. It suggests that educators provide few direct lessons on these concepts, with some perceiving that such lessons are not relevant for young students. Using Bronfenbrenner's framework [7, 8], we recommended ways the HCI community can help integrate privacy and security lessons in school and home settings as well as increase educators' knowledge of digital privacy and security. We also highlighted the need to address broader tensions surrounding the datafication of education. Overall, we see an opportunity for educational technologies to sow the seeds of privacy and security learning among children, and we encourage educators and parents to actively cultivate them.

ACKNOWLEDGMENTS

We thank our participants for sharing their perspectives and Lisa Rogers for assisting with coding the data. We also thank Niklas Elmqvist, Alisha Pradhan, and Daniel Votipka for their feedback on an earlier draft of this paper. Finally, we thank the anonymous reviewers for their useful insights. This research was supported by a Google Faculty Research Award. No one from Google was involved in the research.

REFERENCES

[1] [n. d.]. CommonSense Media. https://www.commonsense.org/education/reviews/all

[2] [n. d.]. Student Privacy Pledge. https://studentprivacypledge.org/

[3] [n. d.]. Teaching Privacy. https://teachingprivacy.org/

[4] June Ahn, Arturo Salazar, Diana Griffing, Jeff Rick, Rachael Marr, Tamara Clegg, Jason Yip, Elizabeth Bonsignore, Daniel Pauw, Lautaro Cabrera, Kenna Hernly, Caroline Pitt, and Kelly Mills. 2018. Science Everywhere: Designing public, tangible displays to connect youth learning across settings. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*. ACM Press, Montreal QC, Canada, 1–12. https://doi.org/10.1145/3173574.3173852

[5] Peter R. Albion, Jo Tondeur, Alona Forkosh-Baruch, and Jef Peeraer. 2015. Teachers' professional development for ICT integration: Towards a reciprocal relationship between research and practice. *Education and Information Technologies* 20, 4 (Dec. 2015), 655–673. https://doi.org/10.1007/s10639-015-9401-9

[6] Hala Assal, Ahsan Imran, and Sonia Chiasson. 2018. An exploration of graphical password authentication for children. *International Journal of Child-Computer Interaction* 18 (Nov. 2018), 37–46. https://doi.org/10.1016/j.ijcci.2018.06.003

[7] Urie Bronfenbrenner. 1976. The experimental ecology of education. *Educational Researcher* 5, 9 (Oct. 1976), 5–15. https://doi.org/10.3102/0013189X005009005

[8] Urie Bronfenbrenner. 1986. Ecology of the family as a context for human development: Research perspectives. *Developmental Psychology* 22, 6 (Nov. 1986), 723–742. http://psycnet.apa.org/buy/1987-06791-001

[9] Tom Buchanan, Carina Paine, Adam N. Joinson, and Ulf-Dietrich Reips. 2007. Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology* 58, 2 (Jan. 2007), 157–165. https://doi.org/10.1002/asi.20459

[10] Tamara Clegg, Jason Yip, Elizabeth Bonsignore, Jon Froehlich, Leyla Norooz, Seokbin Kang, Virginia Byrne, Monica Katzen, Rafael Velez, Angelisa Plane, Vanessa Oguamanam, and Thomas Outing. 2017. Live physiological sensing and visualization ecosystems: An activity theory analysis. In *Proceedings of the 2017 CHI Conference on Human Factors*

in Computing Systems - CHI '17. ACM Press, Denver, Colorado, USA, 2029–2041. https://doi.org/10.1145/3025453.3025987

[11] Commission on Enhancing National Cybersecurity. 2016. *Report on Securing and Growing the Digital Economy*. Technical Report. National Institute of Standards and Technology, Gaithersburg, MD. i–90 pages. https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

[12] Serge Egelman and Eyal Peer. 2015. Scaling the security wall: Developing a security behavior intentions scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 2873–2882. https://doi.org/10.1145/2702123.2702249

[13] Federal Trade Commission. 2018. Child Identity Theft. https://www.consumer.ftc.gov/articles/0040-child-identity-theft

[14] Fordham University. 2012. Privacy Education. https://www.fordham.edu/info/24071/privacy$_{e}$ducation

[15] Andrew Giambrone. 2015. Can Data Improve Education Without Compromising Privacy? *The Atlantic* (June 2015). https://www.theatlantic.com/education/archive/2015/06/big-data-student-privacy/396452/

[16] Charles R. Graham. 2011. Theoretical considerations for understanding technological pedagogical content knowledge (TPACK). *Computers & Education* 57, 3 (Nov. 2011), 1953–1960. https://doi.org/10.1016/j.compedu.2011.04.010

[17] Paulina Haduong, David Cruz, Leah Plunkett, and Urs Gasser. 2016. *The Internet and You*. Technical Report. Berkman Klein Center for Internet & Society, Cambridge, MA. 1–65 pages. http://dlrp.berkman.harvard.edu/node/94

[18] Drew Harwell. 2018. The New Lesson Plan for Elementary School: Surviving the Internet. *Washington Post* (April 2018). https://www.washingtonpost.com/business/economy/the-new-lesson-plan-for-elementary-school-surviving-the-internet/2018/04/06/8b4a8202-0417-494b-a72b-792221e08e3b$_{s}$tory.html

[19] Samantha Hautea, Sayamindu Dasgupta, and Benjamin Mako Hill. 2017. Youth perspectives on critical data literacies. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 919–930. https://doi.org/10.1145/3025453.3025823

[20] Shellie Hipsky and Wiam Younes. 2015. Beyond concern: K-12 faculty and staff's perspectives on privacy topics and cybersafety. *International Journal of Information and Communication Technology Education (IJICTE)* 11, 4 (Oct. 2015), 51–66. https://doi.org/10.4018/IJICTE.2015100104

[21] Lindsay Kalter and Erin Smith. 2016. ACLU of Massachusetts Encourages Schools to Beef Up Student Data Privacy. *Boston Herald* (March 2016). http://www.govtech.com/education/k-12/ACLU-of-Massachusetts-Encourages-Schools-to-Beef-up-Student-Data-Privacy.html

[22] Matthew J. Koehler, Punya Mishra, Mete Akcaoglu, and Joshua M. Rosenberg. 2013. The technological pedagogical content knowledge framework for teachers and teacher educators. In *ICT Integrated Teacher Education: A Resource Book*. Commonwealth Educational Media Centre for Asia, 2–7.

[23] Matthew J. Koehler, Punya Mishra, Kristen Kereluik, Tae Seob Shin, and Charles R. Graham. 2014. The technological pedagogical content knowledge framework. In *Handbook of Research on Educational Communications and Technology*, J. Michael Spector, M. David Merrill, Jan Elen, and M. J. Bishop (Eds.). Springer New York, New York, NY, 101–111. https://doi.org/10.1007/978-1-4614-3185-5$_{9}$

[24] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2017. 'No telling passcodes out because they're private': Understanding children's mental models of privacy and security online. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (Dec. 2017), 1–21. https://doi.org/10.1145/3134699

[25] Priya Kumar, Jessica Vitak, Marshini Chetty, Tamara L. Clegg, Jonathan Yang, Brenna McNally, and Elizabeth Bonsignore. 2018. Co-designing online privacy-related games and stories with children. In *Proceedings of the 17th ACM Conference on Interaction Design and Children (IDC '18)*. ACM Press, 67–79. https://doi.org/10.1145/3202185.3202735

[26] Yifang Li, Nishant Vishwamitra, Bart P. Knijnenburg, Hongxin Hu, and Kelly Caine. 2017. Effectiveness and users' experience of obfuscation as a privacy-enhancing technology for sharing photos. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (Dec. 2017), 1–24. https://doi.org/10.1145/3134702

[27] Sonia Livingstone. 2006. Children's privacy online: Experimenting with boundaries within and beyond the family. In *Computers, Phones, and the Internet: Domesticating Information Technology*, Robert Kraut, Malcolm Brynin, and Sara Kiesler (Eds.). Oxford University Press, New York, NY, 145–167.

[28] Michelle Lui. 2018. Designing for student interactions: The role of embodied interactions in mediating collective inquiry in an immersive simulation. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*. ACM Press, Montreal QC, Canada, 1–12. https://doi.org/10.1145/3173574.3174027

[29] Michelle Lui, Alex C. Kuhn, Alisa Acosta, Chris Quintana, and James D. Slotta. 2014. Supporting learners in collecting and exploring data from immersive simulations in collective inquiry. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14*. ACM Press, Toronto, Ontario, Canada, 2103–2112. https://doi.org/10.1145/2556288.2557162

[30] Anne-Marie Mann, Uta Hinrichs, Janet C. Read, and Aaron Quigley. 2016. Facilitator, functionary, friend or foe?: Studying the role of iPads within learning activities across a school year. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 1833–1845. https://doi.org/10.1145/2858036.2858251

[31] Joseph A. Maxwell. 2010. Using numbers in qualitative research. *Qualitative Inquiry* 16, 6 (July 2010), 475–482. https://doi.org/10.1177/1077800410364740

[32] Melissa Mazmanian and Simone Lanette. 2017. "Okay, one more episode": An ethnography of parenting in the digital age. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17)*. ACM, New York, NY, USA, 2273–2286. https://doi.org/10.1145/2998181.2998218

[33] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys that listen: A study of parents, children, and Internet-connected toys. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 5197–5207. https://doi.org/10.1145/3025453.3025735

[34] Punya Mishra and Matthew J. Kohler. 2006. Technological pedagogical content knowledge: A framework for teacher knowledge. *Teachers College Record* 108, 6 (June 2006), 1017–1054. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.523.3855&rep=rep1&type=pdf

[35] Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Faith Cranor. 2018. Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration. *Proceedings on Privacy Enhancing Technologies* 2018, 4 (Oct. 2018), 5–32. https://doi.org/10.1515/popets-2018-0029

[36] Mark W. Olofson, Meredith J.C. Swallow, and Maureen D. Neumann. 2016. TPACKing: A constructivist framing of TPACK to analyze teachers' construction of knowledge. *Computers & Education* 95 (April 2016), 188–201. https://doi.org/10.1016/j.compedu.2015.12.010

[37] Leysia Palen and Paul Dourish. 2003. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '03)*. ACM, New York, NY, USA, 129–136. https://doi.org/10.1145/642611.642635

[38] Fabio Pittarello, Gualtiero Volpe, and Massimo Zancanaro. 2017. HCI and education in a changing world: From school to public engagement. In *Proceedings of the 12th Biannual Conference on Italian SIGCHI Chapter (CHItaly '17)*. ACM, New York, NY, USA, 31:1–31:2. https://doi.org/10.1145/3125571.3125576

[39] Janet C. Read and Brendan Cassidy. 2012. Designing textual password systems for children. In *Proceedings of the 11th International Conference on Interaction Design and Children - IDC '12*. ACM Press, Bremen, Germany, 200. https://doi.org/10.1145/2307096.2307125

[40] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2017. Where is the digital divide?: A survey of security, privacy, and socioeconomics. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*. ACM Press, Denver, Colorado, USA, 931–936. https://doi.org/10.1145/3025453.3025673

[41] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman. 2018. "Won't somebody think of the children?" Examining COPPA compliance at scale. *Proceedings on Privacy Enhancing Technologies* 2018, 3 (June 2018), 63–83. https://doi.org/10.1515/popets-2018-0021

[42] Joshua M. Rosenberg and Matthew J. Koehler. 2015. Context and technological pedagogical content knowledge (TPACK): A systematic review. *Journal of Research on Technology in Education* 47, 3 (July 2015), 186–210. https://doi.org/10.1080/15391523.2015.1052663

[43] Johnny Saldañna. 2013. *The Coding Manual for Qualitative Researchers* (2nd ed ed.). SAGE, Los Angeles.

[44] Natasha Singer. 2017. How Google Took Over the Classroom. *The New York Times* (May 2017). https://www.nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html

[45] Aaron Smith. 2017. *What Americans Knows About Cybersecurity*. Technical Report. Pew Research Center, Washington, DC. http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/

[46] Hiller Spires, Eric Wiebe, Carl Young, Karen Hollebrands, and John Lee. 2012. Towards a new learning ecology: Professional development for teachers in 1:1 learning environments. *Contemporary Issues in Technology and Teacher Education* 12, 2 (June 2012), 232–254. https://www.learntechlib.org/p/35450/

[47] Hiller A. Spires, Kevin Oliver, and Jenifer Corn. 2011. The new learning ecology of one-to-one computing environments. *Journal of Digital Learning in Teacher Education* 28, 2 (Dec. 2011), 63–72. https://doi.org/10.1080/21532974.2011.10784682

[48] Hiller A. Spires, Eric Wiebe, Carl A. Young, Karen Hollebrands, and John K. Lee. 2009. *Toward a New Learning Ecology: Teaching and Learning in 1: 1 Environments*. Technical Report Number One. The William & Ida Friday Institute for Educational Innovation at the North Carolina State University College of Education, Raleigh, NC. 1–25 pages. http://www.unc.edu/world/toward-a-new-learning-ecology(12).pdf

[49] Valerie Steeves. 2010. Online surveillance in Canadian schools. In *Schools Under Surveillance: Cultures of Control in Public Education*, Torin Monahan and Rodolfo Torres (Eds.). Rutgers University Press, New Brunswick, 87–103. http://muse.jhu.edu/chapter/139714

[50] Valerie Steeves. 2010. *Summary of Research on Youth Online Privacy*. Technical Report. Office of the Privacy Commissioner of Canada, Ottawa, Canada. https://priv.gc.ca/media/1731/yp$_2$01003$_e$.pdf

[51] Lajeane G. Thomas and Donald G. Knezek. 2008. Information, communications, and educational technology standards for students, teachers, and school leaders. In *International Handbook of Information Technology in Primary and Secondary Education*, Joke Voogt and Gerald Knezek (Eds.). Springer US, Boston, MA, 333–348. https://doi.org/10.1007/978-0-387-73315-9$_2$0

[52] Joke Voogt and Gerald Knezek. 2008. IT in primary and secondary education: Emerging issues. In *International Handbook of Information Technology in Primary and Secondary Education*, Joke Voogt and Gerald Knezek (Eds.). Springer, New York, xxix–xxlii.

[53] Yang Wang, Pedro Giovanni Leon, Kevin Scott, Xiaoxuan Chen, Alessandro Acquisti, and Lorrie Faith Cranor. 2013. Privacy nudges for social media: An exploratory Facebook study. In *Proceedings of the 22nd International Conference on World Wide Web - WWW '13 Companion*. ACM Press, Rio de Janeiro, Brazil, 763–770. https://doi.org/10.1145/2487788.2488038