"We picked community over privacy": Privacy and Security Concerns Emerging from Remote Learning Sociotechnical Infrastructure During COVID-19

KELLY B. WAGMAN, University of Chicago, USA
ELANA B. BLINDER, University of Maryland, USA
KEVIN SONG, University of Chicago, USA
ANTOINE VIGNON, University of Maryland, USA
SOLOMON DWORKIN, University of Chicago, USA
TAMARA CLEGG, University of Maryland, USA
JESSICA VITAK, University of Maryland, USA
MARSHINI CHETTY, University of Chicago, USA

With the rapid shift to remote learning in the early days of the COVID-19 pandemic, parents, teachers, and students had to quickly adapt to what scholars have called *emergency remote learning* (ERL). This transition required increased reliance on digital tools, exacerbating privacy and security threats associated with expanded data collection and new vulnerabilities. In this study, we adopt a sociotechnical and infrastructural perspective to understand how these threats emerged through breakdowns and tensions in elementary school ERL. Through interviews with 29 US-based teachers and parents of elementary school students (grades PreK-6), we identify two core findings related to privacy and security. First, we detail three breakdowns in the ERL sociotechnical infrastructure: (1) reduced attention to privacy and security issues as parents and teachers cobbled together a patchwork of tools needed to make ERL work; (2) privacy and security risks that emerged from ambiguous and shifting school policies; and (3) the failure to adapt standard authentication mechanisms (e.g., passwords) to be usable by young children. Second, we identify tensions between parents' and teachers' desire to help children advance in their education and their desire for children's privacy and security in ERL, as well as tensions resulting from the collapse of home and school contexts. These findings collectively suggest that ERL exacerbated existing—and created new—privacy and security challenges for young students, and we argue these challenges will carry beyond the pandemic due to the increasing use of technology to supplement traditional education. In light of these findings, we recommend researchers and educators use a *framework of care* to develop social and technical approaches to improving remote learning in order to protect children's privacy and security.

CCS Concepts: • **Human-centered computing → Empirical studies in collaborative and social computing**.

Additional Key Words and Phrases: emergency remote learning, education, children, teachers, privacy, security, sociotechnical infrastructure, science and technology studies, STS, COVID-19

Authors' addresses: Kelly B. Wagman, University of Chicago, Chicago, IL, USA; Elana B. Blinder, University of Maryland, College Park, MD, USA; Kevin Song, University of Chicago, Chicago, IL, USA; Antoine Vignon, University of Maryland, College Park, MD, USA; Solomon Dworkin, University of Chicago, Chicago, IL, USA; Tamara Clegg, University of Maryland, College Park, MD, USA; Jessica Vitak, University of Maryland, College Park, MD, USA; Marshini Chetty, University of Chicago, Chicago, IL, USA.

2573-0142/2023/10-ART245 $15.00
https://doi.org/10.1145/3610036

ACM Reference Format:
Kelly B. Wagman, Elana B. Blinder, Kevin Song, Antoine Vignon, Solomon Dworkin, Tamara Clegg, Jessica Vitak, and Marshini Chetty. 2023. "We picked community over privacy": Privacy and Security Concerns Emerging from Remote Learning Sociotechnical Infrastructure During COVID-19. *Proc. ACM Hum.-Comput. Interact.* 7, CSCW2, Article 245 (October 2023), 29 pages. https://doi.org/10.1145/3610036

1 INTRODUCTION

The COVID-19 pandemic caused a widespread shutdown of schools around the globe and necessitated a transition from in-person schooling to *emergency remote learning*[1] (ERL) unexpectedly and for an extended period of time [67]. In 2020, ERL was the primary form of schooling in the United States, with nearly all U.S. parents (93%) saying their children engaged in some form of remote learning during the first year of the pandemic [67]. Privacy and security concerns emerged during this period as researchers and the press highlighted how the increased use of digital tools in education led to issues such as exposure to inappropriate content through Zoombombing[2] and the misuse of personal data [1, 30, 32, 39, 41, 43, 45, 52, 67, 76].

In this paper, we focus on the privacy and security concerns impacting elementary school children during ERL. We build on prior work finding that young children are particularly vulnerable to privacy and security threats because of their relative lack of experience with online tools, their limited mental models of privacy and security issues and threats, and because adults structure most of their lives so the burden of dealing with these issues has not typically fallen to them alone [25, 34, 37, 44, 49, 82]. We also extend recent research exploring aspects of privacy and security in ERL [30, 76], and we argue that the CSCW community is especially well-positioned to address this topic due to the sociotechnical challenge ERL presents. Evaluating these issues is critical for improving digital privacy and security for children in educational settings.

Despite the fact that by late 2021 the majority of students were back to attending school in-person [61], the year—or more—spent remote provides a useful case study for identifying privacy and security issues that emerge when digital tools are used in elementary education. On the one hand, this case study can provide insight into how privacy and security issues might continue to surface as elementary schools increasingly adopt new digital teaching tools to structure and supplement in-person learning. On the other hand, it can improve our understanding of how to design ERL systems to better manage children's privacy and security so that when future crisis situations arise—and require a switch to remote learning—we are ready.

To accomplish this goal, this paper evaluates how privacy and security concerns impacting elementary school children were exposed during ERL. We draw on work in CSCW and Science and Technology Studies (STS) to frame ERL as a sociotechnical system [31, 72]. Doing so allows us to understand ERL as a nuanced, complex, and evolving system comprised of both social and technical relations including tools, policies, and stakeholder relationships. We consider these social and technical relations as the infrastructure that makes up the system [31, 72] through which privacy and security emerge, not as stable concepts, but dependent on the *"particular social and cultural circumstances"* [16] (p. 335) of the system. Said another way, neither privacy nor security are states that can be fully achieved; rather, they represent boundaries that are always under negotiation [16].

ERL presents a case to examine the negotiation of privacy and security in the context of elementary education. Within CSCW, however, we are not just interested in how these concepts are

[1]Emergency remote learning differs from traditional remote learning because it is not planned in advance, but is instead the result of rapidly moving in-person learning to an online format [11, 21, 30]. ERL is also sometimes called *emergency remote education* or *emergency remote teaching*.
[2]Zoombombing is when an intruder joins a video call with the intention of causing disturbance, typically through the display of inappropriate content [39].

negotiated but in paths to improving the design of the system. Some STS scholars have argued for understanding how to improve or repair a sociotechnical system by identifying points of *breakdown* in need of attention [28]. Another approach is to look at how *tensions* emerge that question or shift how stakeholders in the system see the goal of privacy and security for children [26, 54, 62]. Thus, to understand how to improve the sociotechnical privacy and security infrastructure for elementary school children in ERL, we also need to know where breakdowns and tensions exist to suggest improvements for the future. In our work, we asked two primary research questions:

RQ1: What *infrastructure breakdowns* surfaced during ERL in elementary education that led to privacy and security concerns?

RQ2: What *privacy and security tensions* emerged or were exacerbated during ERL in elementary education?

To answer these questions, we conducted semi-structured interviews with 29 elementary school (PreK-6) teachers and parents in the U.S. during 2021, one year into the pandemic, following a full year of remote learning. We spoke with participants about their experiences with remote learning during the pandemic, focusing on both social and technical challenges associated with helping elementary school children use technology to attend school from home, and the privacy and security concerns and issues that resulted from ERL.

Our two main findings reflect participants' experiences with PreK-6 ERL during the COVID-19 pandemic. First, infrastructural breakdowns that led to privacy and security issues included: (1) an overwhelming patchwork of tools needed to make ERL function; (2) ambiguous and shifting school policies; and (3) a lack of authentication infrastructure designed for young children. Second, privacy and security tensions emerged between the desire to ensure children were learning online and concerns about increased parent/teacher and institutional surveillance, as well as around the appropriate roles of parents and teachers in ERL as home and school boundaries blurred during synchronous remote learning.

In our discussion, we develop a theoretical framework for understanding privacy and security in the context of elementary school ERL. First, we argue that ERL during the pandemic can be characterized as a *contingent sociotechnical system*—a term we contribute—given its unforeseen circumstances, rapid development and deployment, and brittle, precarious nature. ERL in this framing was comprised of a complex web of technologies and ongoing labor performed largely by parents and teachers to maintain children's learning, socialization, and privacy and security. When privacy and security for elementary school children are considered via this sociotechnical lens, it becomes clear that their deprioritization during system-building is a systemic rather than individual issue.

We further consider how privacy and security labor in this context is a form of care. For young children in particular, a critical part of the educational process enacted by parents and teachers is to watch children to keep them safe and correct their behavior or enforce classroom rules and discipline; Steeves and Jones [74] refer to this as *"surveillance as care,"* a point echoed in other work [46]. Using this lens of care helps to view tending to the security of information technology systems—and privacy and security more generally—as a process of ongoing human maintenance that does not have a one-time technical solution [33]. Moreover, developing *care infrastructure* can be a vehicle to support the privacy and security of vulnerable populations, including children, by centering their well-being [77]. We build on this literature by considering how the development of educational privacy and security infrastructure could be reframed and reoriented using the lens of caring for young children.

Our paper contributes a nuanced sociotechnical and infrastructural picture of privacy and security challenges connected to ERL for young children and, in doing so, continues the long tradition

in CSCW of situating technical questions in their social and organizational contexts. Our key contributions include: (1) surfacing breakdowns in ERL that parents and teachers deemed important for children's privacy and security and making concrete recommendations for how researchers can use these as starting points for design; (2) highlighting privacy and security tensions in ERL that illuminate how these concepts are being negotiated by stakeholders as digital tools are increasingly a part of elementary education; (3) developing the concept of the *contingent sociotechnical system* to describe ERL and applying the idea of privacy and security as a form of *care* to the educational context for the first time; and (4) providing design implications for the CSCW community and educators, designers, and policymakers.

2 RELATED WORK

In this section, we describe prior work examining privacy and security issues for children in education, ERL during the COVID-19 pandemic, and how privacy and security can be viewed as a form of care for young children.

2.1 Privacy and Security Issues for Children in Education

Our work contributes to a growing body of research devoted to understanding children's online privacy and security perceptions, challenges, and needs [29, 34, 37, 44, 60, 81, 82, 84, 85]. One area of this research looks at possible harms children face online. Some research suggests elementary-aged children are particularly vulnerable to cyber threats insofar as their comfort experimenting with new technologies often exceeds their critical understanding of the associated risks [44, 81]. Researchers have identified specific threats such as misuse of private information, phishing, and cyber bullying [45, 76] and investigated how children themselves understand collection of their data [80, 82].

A second area of work explores the extent to which teachers and parents—the primary adult stakeholders in children's education—are equipped to protect and prepare children to navigate online privacy and security issues perceived as important based on prior research (e.g., helping children make strong passwords). Researchers have largely concluded that teachers and parents are under-prepared to help children with these issues. For example, in pre-pandemic studies, elementary teachers rarely reported having received relevant training in privacy and security education or teaching formal lessons on these topics with their students [4, 36, 48], let alone in online instruction [53]. These studies also suggest that both teachers and parents lacked general media literacy and protective strategies for children's online privacy prior to the COVID-19 crisis [44]. Stemming from this lack of educational content about privacy and security, researchers have designed pedagogical resources for educating young learners about privacy and security, including through novel formats such as comics [50], games [35, 49], and social robots [9].

Only a few studies have focused on understanding privacy and security concerns for children during ERL amidst the COVID-19 pandemic. While digital technology was already pervasive and deeply embedded in children's lives at school/home prior to the pandemic [36, 47, 55], it became more prevalent during ERL, resulting in an increase in the number and type of threats encountered by children, teachers, and parents [30, 45, 76]. Tazi et al. [76] and Lobe et al. [45] both conducted large-scale surveys to identify threats to children (all ages and ages 10–18, respectively) related to privacy and security during ERL such as student data leaks, screen overuse, cyberbullying, phishing, and disinformation. This work was not focused on young children, however, and did not include qualitative interview data. Our approach is most similar to a study by John et al. [30], who also use a STS lens to understand privacy in ERL. Their study compares how cultural conceptions of privacy influenced ERL in Germany and Israel; they find, for example, that while Israel quickly adopted mostly American commercial technology for ERL without strong privacy considerations

(e.g., Zoom), Germany tended to be more privacy-aware and focused on adhering to General Data Protection Regulation (GDPR), which meant using fewer tools from 'big tech.'

Our study also uses a STS lens to understand how privacy and security are negotiated in ERL, although we are focused on elementary school ERL in the U.S. and, instead of a comparative analysis, we contribute to this body of work by identifying points of breakdown/tension in the ERL sociotechnical system. Since we are situated within CSCW and human-computer interaction (HCI), our goal is also to point toward future possibilities for design and intervention to enhance digital privacy and security for young children in learning environments and more broadly. Our work differs both from previous work that identifies specific threats as well as studies on pedagogy by contextualizing privacy and security concerns in education within a sociotechnical and infrastructural framework. This allows us to identify aspects of the root causes of privacy and security concerns within ERL and how they might be addressed systemically, as opposed to at an individual or pedagogical level.

2.2 Emergency Remote Learning Infrastructure During the COVID-19 Pandemic

The learning sciences community has investigated social and pedagogical aspects of remote learning infrastructure since before the recent proliferation of online and hybrid classrooms due to the COVID-19 pandemic [65, 68]. Scholars have discussed remote learning challenges including how remote instruction requires access to technology, skills, and support systems that are not uniformly available to all children [3, 8]. These challenges were amplified during the rapid scaling of fully online education in 2020, necessitated by the lockdowns and social distancing mandates. Education researchers have noted how the emergency nature of this context left little room for the careful planning and forethought required for the design of meaningful online learning experiences for children [5, 11, 12, 24] and therefore relied heavily upon the trial and error approaches of teachers, the majority of whom lacked experience in online teaching [2, 15, 22, 63]. These studies describe how ERL also depended on the support of parents and other family members whose experience with technology and availability to support their children during synchronous lessons varied dramatically [2, 22]. Some studies show how many U.S. school districts supplied tablets and laptops to students for home use to counter digital divide-related discrepancies in students' connectivity and technology access; such efforts often fell short of addressing the needs of families in resource-constrained communities lacking broadband and other forms of support [53, 64, 71]. Other scholars have also identified privacy issues for ERL in higher education such as university student concerns about camera use during remote learning [23, 41] as well as a negative correlation between perceived usefulness of large-scale learning analytic platforms and ability to protect student privacy [42].

Within CSCW and HCI, a few researchers have studied the technical aspects of ERL infrastructure and the social interactions with this infrastructure, although relatively few of these studies pertain specifically to elementary school education [57, 78]. For instance, some researchers experimented with how to improve school participation during ERL with elementary and middle school students [51] while others looked at parents' role in education during the pandemic [56, 83]. Several papers illuminate aspects of ERL sociotechnical infrastructure that have relevance for privacy and security concerns [12, 21, 30, 83]. Cumbo et al. and Ewing et al. [12, 18] studied the ERL experiences of families with young children in Australia and note how the fusion of the home and school environment can both give parents insight into their children's learning and also lead to discomfort from observing struggling teachers and negotiating their own involvement in their children's education. A similar study by Gui et al. [21] interviewed teachers and guardians of K-12 students in China, finding that invisible collaborative labor performed by these groups was critical for the functioning of ERL. In this work, Gui et al. also provide evidence of how Chinese culture impacted the country's ERL sociotechnical system by highlighting how the hierarchy between teachers and

guardians often posed an obstacle to collaboration. As already noted, John et al. [30] examine privacy and security issues with respect to ERL during the pandemic in Israel and Germany.

These studies paint a portrait of how families and teachers experienced ERL and associated technologies during the pandemic; however, they do not consider the extent to which such strategies addressed or contributed to privacy and security challenges for elementary education or focus on the U.S. more deeply as we do in our work. Specifically, we build upon Cumbo et al. [12] and Gui et al.'s [21] findings regarding the challenges associated with the surveillance of teachers by incorporating an examination of data collected by institutions and corporations (see, for example, [44, 70]) and privacy concerns related to the surveillance of students' home environments and extracurricular online activities.

2.3 Privacy and Security as Care Infrastructure

Prior work in CSCW and HCI has framed privacy and security as a form of care infrastructure [33, 77]. Specifically, in the domain of education, Lu et al. [46] have explained the work of managing student data by teachers as a tension between enacting care and control. Within this tension, on the one hand, teachers have a desire and a responsibility to care for children and protect them from harm. On the other hand, teachers can also act as surveillant consumers [73], using data to control student engagement, track learning, and increase time-on-task during school [21, 36, 38], complicating their role as safeguarders of students' privacy. Similarly, prior work showed that even before COVID-19, parents often surveilled their children's online activity using apps, in-person monitoring, and by reviewing content directly on their children's devices in order to regulate screen time and prevent access to age-inappropriate content [34, 55, 70, 74, 79]. In our paper, we build on this work by attuning to the ways that parents and teachers navigate the tension between care and control with respect to surveillance during ERL.

To highlight a path toward improving sociotechnical infrastructure, scholars in CSCW have advocated for addressing system breakdowns through care and repair work (e.g., [28, 31]). We take inspiration from this framework given that privacy and security concerns for children are situated within complex systems and competing stakeholder priorities (e.g., in the case of care versus control). We therefore frame our work as identifying and addressing tensions/breakdowns as well as *care*-based interventions in order to envision a way to better protect children from privacy and security threats while continuing to acknowledge the nuance and complexity of these systems.

3 METHODS

To address our research questions, we conducted semi-structured, virtual (Zoom) interviews with U.S. adults who were PreK-6 parents and/or teachers of PreK-6 students who underwent remote learning in the 2020-2021 school year due to the COVID-19 pandemic.[3] We chose to obtain perspectives from two key stakeholder groups involved in elementary education and learning because it provides a form of data triangulation [13], enabling us to develop a more robust and holistic understanding of the privacy and security challenges ERL created and exacerbated. We also note that while we would have preferred to collect experiences from students themselves, we chose not to because of the significant restrictions placed on in-school access and the broader challenges in speaking with parents and teachers during the pandemic.

We also want to note the research team's background and how it influenced the study design. This paper is part of a wider project on privacy and security education opportunities for young

[3]Most elementary schools in the U.S. are K-5 but in some locations, PreK and/or 6th grade are also considered elementary school. Given challenges with recruitment, we used the broader grade range.

children.[4] The research team, which includes three faculty members, two PhD students, and several additional graduate and undergraduate students at any given time, spans HCI, Learning Sciences, Communication, and STS. Two faculty members are subject matter experts on usable privacy and security, while the third is a subject matter expert on designing with and for children. Team members also offer perspectives as a former elementary school teacher (one member) and as a parent of young children (one member). While we do not include our own experiences directly in the paper, we make visible these perspectives as a way of acknowledging our positionality.

3.1 Data Collection

After receiving approval from our Institutional Review Board (IRB), we began recruiting teachers and parents through social media in December 2020, including personal networks on Facebook and Twitter, as well as approved posts in Facebook groups focused on elementary school education and institutional mailing lists pertaining to PreK-12 education. Prospective interview participants were asked to complete a short survey (included in supplementary Appendix **??** and **??**) regarding their teaching and/or parenting experiences related to ERL, demographic information, and, in the case of teachers, information on their teaching environment. Survey respondents who met our criteria for participation—U.S. adults who were either the parent of a PreK-6 student or taught in an elementary school that participated in ERL—were contacted via email to schedule an interview. Interviews were conducted over a nine-month period between December 2020 and September 2021.[5]

Parents and teachers had separate interview protocols (included in supplementary Appendix **??** and **??**), although both were structured around our primary research questions, focusing on their experiences transitioning to ERL and navigating privacy and security challenges in the remote learning environment. Specifically, interviews were organized into three sections to help us identify tensions around privacy and security and breakdowns in ERL, including: (1) experiences with online schooling/learning; (2) experiences related to privacy and security in remote learning; and (3) opportunities for future privacy and security learning. We tailored teacher questions to capture teaching-specific experiences, such as challenges around remote learning technologies, managing children's privacy and security in remote learning, and conversations they had around these topics with parents and students, if any. We also asked if teachers included any online privacy and security topics in their daily interactions with students. We asked parents how they managed remote schooling and set up specific routines with their child(ren), including rules around technology use and to maintain privacy and security in remote learning. Once we had draft interview guides, we conducted pilot interviews with two parents and three teachers, using each pilot to refine our questions and wording. We did not include these pilot interviews in our final data set.

Each interview was audio recorded and lasted between 30-60 minutes. Each participant received a US$25 Amazon gift card upon completing the interview. We continued interviewing teachers and parents until we did not hear new themes; at that point, we determined we had reached data saturation and stopped collecting data [66].

3.2 Data Analysis

Interviews were uploaded and transcribed through Rev.com under a non-disclosure agreement. We used MAXQDA qualitative analysis software to qualitatively code interview transcripts. We analyzed the data through iterative, deductive coding and thematic analysis, following the processes outlined by Saldaña [66] and Braun and Clarke [6, 7] to identify and organize patterns in the data.

[4]Full project details and publications can be found at https://SPE4K.umd.edu.

[5]We faced significant challenges to recruiting participants, likely due to the added stress and reduced support parents and teachers faced during the height of the pandemic, which lengthened the data collection period.

Table 1. Partial codebook, with descriptions for subset of codes used in this paper's analysis. Structural codes are bolded.

Code	Code Description
Day In the Life Remote Learning	
Remote learning challenges	Challenges from using technology for remote learning
Remote learning tools	Describing use of educational technology and classroom management tools during ERL
Parent communication (teachers only)	How teachers communicated with parents during ERL
Uncomfortable moments	Examples of uncomfortable, awkward, or unexpected privacy/security incidents in remote learning
Privacy and Security Issues	
Student data collection	Types of information teachers/parents thought was being collected/used as part of ERL
Privacy and security concerns	Challenges teachers/parents faced navigating and managing digital privacy and security
Privacy and security non-concerns	Issues of non-concern around privacy and security
Decisions about camera use	Decisions about camera use during ERL
Privacy and security tools	Tools teachers/parents use to achieve privacy and security
Privacy and security norms	Examples of privacy and security etiquette and behaviors teachers/parents shared with children
Privacy and security management	Examples of rules teachers/parents enforced regarding technology use to protect children's privacy and security
Sharing student information (teachers only)	How teachers decide what information to share about themselves and about students with parents

First, the full research team developed an initial codebook using three organizing structural codes [66] that were informed by the research questions and interview protocols: *'day in the life of remote learning,' 'privacy and security related issues,'* and *'future learning opportunities.'* We then iteratively coded a subset of interviews; this process involved multiple team members coding one or more transcripts and identifying sub-codes for each structural code, then meeting as a team to discuss and update the codebook. For example, subcodes generated from these discussions included 'remote learning benefits,' 'student data collection,' and 'existing school micro-lessons.'

We initially created separate codebooks for parents and teachers, but after examining the codes and subcodes, it became evident that the codes were highly similar, so we created a master codebook to use on all the transcripts. Given that parents and teachers represent two key stakeholders within the ERL system, it is unsurprising that both groups shared examples of breakdowns and tensions in this unified sociotechnical system. The final codebook had three main codes and 23 subcodes; in this analysis, we focus on a subset of two main codes / 12 subcodes (see Table 1). Through this process, we found that many systems-level concerns were shared by parents and teachers, but in presenting our findings, we explicitly note when one group had a unique perspective.

Each transcript was then coded twice in MAXQDA using the finalized codebook: first, one member read and applied codes/subcodes to a transcript, then a second member reviewed the transcript to ensure we captured all relevant excerpts. We then exported excerpts for each of these codes to further analyze, identify trends, and write detailed summaries as described in phase three of Braun and Clarke's [6, 7] reflexive thematic analysis process. During the second cycle of coding, team members were assigned specific codes and read all excerpts associated with a given code to identify patterns or categories across the data. They then wrote an analytic memo for each code [66], describing the patterns and including representative quotes. The full team reviewed and

discussed these memos, grouping categories together to reveal overarching themes that informed our research questions. Aligning with Braun and Clarke's [6, 7] phases four and five of thematic analysis, the research team reflectively questioned, critiqued and iterated on the developed themes to further define them. Through this process, we converged on the final themes discussed in our findings relating to emergency remote learning and privacy and security concerns.

Participant names have been replaced with alpha-numeric identifiers to protect their identity. We denote participants who were teachers with the letter 'T' and participants who were parents with the letter 'P.'

3.3 Participants

In total, we interviewed 16 parents and 17 teachers. Four interviews were excluded due to questions related to participant legitimacy (e.g., cases where participants' claimed to be teachers but their responses suggested they were not), resulting in 29 interviews included in our analysis (15 parents, 14 teachers). Table 2 provides an overview of our participants' background and technology use during ERL.

Nearly all teachers we spoke to were women, although there was significant racial diversity, with just three people identifying as white (and the largest subset, n=8, identifying as multiracial). They were largely from the Mid-Atlantic region, with just two living in other parts of the US. All teachers we spoke to worked at public elementary schools (with the exception of T16 who taught 6th grade, which was considered middle school in their district); they had been teaching for 4-30 years and spanned all grades from pre-kindergarten through sixth grade (ages 4-12). We also asked teachers about the technology they used to supplement and complement their remote teaching, providing them with a list of 25 popular tools. Our participants used a wide range of technologies to support their teaching, with the most popular tools being Google Drive (n=14), Google Meet (n=12), YouTube (n=12), Zoom (n=10), Starfall (n=7), and ClassDojo (n=7) (see a full list of tools in Appendix 7.1). In addition, we asked whether teachers had experienced "Zoombombing"—when an unauthorized participant joins an online video call in a disruptive manner—in their classroom as a baseline metric for understanding ERL security threats. Four reported experiencing Zoombombing.

The parents we spoke to were also primarily women, but were more geographically diverse than teachers, living in all major regions of the country.[6] There was also more diversity in the type of school parents sent their children to, although the majority (n=11) attended public school. Nine parents had multiple children, but in the interviews we asked them to focus on their youngest PreK-6 child. We asked parents several questions about technology monitoring procedures in order to gather baseline information related to privacy and security preferences. Only two parents (P1, P14) had downloaded apps to monitor their child's device use, but most had rules about how long their child could use devices (n=9) and which sites/apps they could access (n=13).

Finally, given the privacy concerns associated with camera use inside the home, we asked teachers and parents about requirements for students to have their camera on while in virtual class. Among teachers, there was a mixed response: eight said yes (they require camera use), four said no (they do not require camera use), and two said it depends. Among parents, all said their child always or sometimes had their camera on while in remote class.

[6]We did not collect race data from parent participants.

Table 2. Participants: Demographics and Technology Use.

Teacher ID	Gender	Region	School	Grades*	#Yrs Teaching	Zoombombed?	Camera On**
T1	F	Mid-Atlantic	Public	PreK	10	No	Yes
T3	F	Mid-Atlantic	Public	2	8	No	Yes
T4	F	Mid-Atlantic	Public	2	4	No	No
T5	F	Mid-Atlantic	Public	K-5	9	No	Yes
T6	F	Mid-Atlantic	Public	Prek-5	8	No	No
T7	F	Mid-Atlantic	Public	3	8	Yes	Yes
T8	F	Mid-Atlantic	Public	K	16	No	It Depends
T9	F	Mid-Atlantic	Public	PreK-5	20	Yes	Yes
T10	F	Mid-Atlantic	Public	K	13	Yes	No
T11	F	Mid-Atlantic	Public	PreK	30	No	Yes
T12	F	Northeast	Public	1	19	No	Yes
T15	F	Mid-Atlantic	Public	K	8	No	It Depends
T16	M	Midwest	Public	6	11	No	Yes
T17	F	Mid-Atlantic	Public	PreK	5	Yes	No
Parent ID	**Gender**	**Region**	**School**	**Grades***	**Time Limit*****	**Restrictions*****	**Camera On****
P1	F	Southwest	Public	3	Yes	Yes	Always
P2	F	Midwest	Public	1, 4	Yes	Yes	Sometimes
P3	F	Northeast	Public	4, 6	No	No	Always
P4	M	Northwest	Charter	1	Yes	Yes	Always
P5	F	Southwest	Magnet	PreK, 1	No	Yes	Always
P6	F	Mid-Atlantic	Public	1, 4	No	Yes	Always
P7	F	Not reported	Private	K	Yes	Yes	Always
P8	F	Mid-Atlantic	Public	2, 6, 10	No	Yes	Always
P9	F	Mid-Atlantic	Public	5	Yes	No	Sometimes
P10	F	Southwest	Public	1	Yes	Yes	Always
P11	F	Midwest	Public	K	Yes	Yes	Always
P12	F	West	Public	1, 3	Yes	Yes	Sometimes
P13	F	Midwest	Public	PreK, 1	No	Yes	Sometimes
P14	M	West	Public	5, 9	No	Yes	Sometimes
P16	F	Mid-Atlantic	Charter	PreK, 1	Yes	Yes	Not reported

Notes: T denotes teachers, P denotes parents. Only teachers were asked about whether they experienced any incidents of Zoombombing

*Teachers were asked what grade(s) they taught; parents were asked what grade(s) their children were in.

**Teachers were asked if they require students have cameras on during class; parents were asked if their children turn on their camera when in class.

***Parents were asked whether they limit how long their children can use devices and if they restrict which apps or websites their children can access.

4 FINDINGS

In this section, we organize our findings by our two research questions: identifying elementary school ERL *breakdowns* and *tensions* experienced by teachers and parents. First, we describe breakdowns in the sociotechnical components of ERL infrastructure that emerged as important with respect to privacy and security concerns for elementary school students. Second, we describe how tensions around surveillance and the collapse of home and school contexts arose during ERL and put into question existing social norms for students, parents, and teachers.

4.1 RQ1: ERL Infrastructure Breakdowns Led to Privacy and Security Concerns for Elementary School Children

Breakdowns allow us to see where ERL falls apart and thus where it is in need of repair. In this section, we focus on three types of breakdowns that emerged from our data that created or

exacerbated online privacy and security concerns for elementary children, parents, and teachers owing to (1) the patchwork of ERL digital tools and communication channels needed to make ERL work (4.1.1), (2) shifting school policies (4.1.2), and (3) the lack of standard authentication mechanisms, especially for young children (4.1.3). We describe participants' experiences with these breakdowns, as well as the privacy challenges they raised for students, parents, and teachers, and how parents and teachers worked to resolve these breakdowns to keep ERL functioning.

4.1.1 The Overwhelming Patchwork of Tools Needed for ERL Added Burden and Necessitated Altered Policies On Home-School Communications. Teachers and parents we spoke to told us they and their students were overwhelmed by the sheer quantity of remote learning tools available and how often they moved from one tool to another during ERL. Participants named more than 80 tools they used during ERL, including tools for video calling, tracking assignments and grades, communication, and learning activities. Our participants reported that many interactions that were previously done in-person now required a host of both new and known technologies; for example, T9 said, *"[The students] suffered from technology bombardment. I just coined that. I just named that because it became like, use this and this and this and this."* The learning curve for this "technology bombardment" could be steep. P14, the parent of a 5th grader, said, *"I think the biggest struggle is that all of a sudden all the students and all the teachers had to learn all these programs, and so as they were kind of getting started, there is a big struggle for teachers to adapt."*

The patchwork of educational and communications tools—along with efforts by parents, teachers, and students to use them—is a key part of the sociotechnical infrastructure needed for ERL; however, the use of these tools also often meant stakeholders, including parents, teachers, and students, had to sacrifice privacy to make ERL work. For example, participants' comments about parent-teacher communication—especially early in the pandemic when there was significant uncertainty and confusion about best practices and policies—highlight these increased privacy risks around disclosing personal information and methods of contact.

Our participants described how the overwhelming task of building up a piecemeal set of tools for ERL constituted a breakdown in infrastructure and led to privacy and security for students, parents, and teachers being deprioritized in favor of getting students online and learning. Both participant groups mentioned they had questions such as *How am I going to get a 5-year-old on Zoom? How long will remote learning last?* with no answers forthcoming. Given this uncertainty and confusion about how to make ERL work or how long ERL would last, teachers and parents had to make tough choices to keep students learning; as T7 noted, one decision they made was to choose "community over privacy:"

> *When COVID first happened, we picked community over privacy to a certain degree, in the sense that for the teachers, we were giving out our phone numbers, our personal cell phone numbers because that was the only way we could really communicate, because email just wasn't efficient, especially with a lot of the Spanish speaking families, or just people who don't have wifi that much. So, we did have to compromise on that.*

This teacher captures a feeling shared by numerous participants that privacy and security were valued, but ultimately overlooked because getting the ERL sociotechnical system to function at all was challenging enough. Some teachers elaborated that they shared personal contact information with families because they were concerned that some families could not easily access email for school communications. As T17 noted, *"I text all my families. It's the easiest way to get in touch with them. I find that that's way more accessible than email for a lot of my families. ...sometimes that access is a big deal for them. So texting and calling are way easier."*

That said, while texting and calling may have been accessible to more families and learners, participants spoke of how this required teachers to share their personal phone number—something

teachers were not always comfortable doing and which they may not have chosen to do pre-pandemic. To deal with this discomfit, some teachers developed ways of communicating with parents during ERL while keeping their contact information private. Several teachers said they used Google Voice, which obfuscates the actual phone number, including T3, who said, *"With parents, I use Google Voice to text with them so they don't have my actual number. And I also use an email with the parents, for the ones who check it. In this day and age, we're mostly texting. That's the most response that I get from parents."* Using Google Voice—which allowed teachers to balance their accessibility to families and privacy considerations—was just one strategy we observed in our data. Other teachers adopted different online tools to maintain their own privacy from parents while still maintaining appropriate levels of contact with students and their families. T4 was one of seven teachers who used ClassDojo, a popular educational tool, to communicate with parents; they said, *"I'd call [ClassDojo] a social media app. But it is obviously restricted and private... that's how I can text parents and they can text me without them actually knowing my phone number."*

As these communication systems solidified during ERL over time, teachers told us they selected a communication channel based on what information they wanted to share with parents. They primarily used email to share assignments, class updates, and schedules; text messages for quick updates and reminders; and calls for emergencies such as absences and personal issues or concerns. In our data, it became clear that parent-teacher communication was critical for making ERL work for young learners through supporting their families. Yet, because this communication needed to be done remotely, it necessitated the use of a collection of tools by students, parents, and teachers as well as new forms of teacher and parent labor to make the system work. The new channels of parent-teacher communication needed in ERL in particular stretched privacy norms around information disclosure and methods of contact and was especially challenging when private contact information had to be exchanged between teachers and families to stay in touch.

4.1.2 Ambiguous and Shifting School Privacy/Security Policies. Our data highlight that school policies played an important role in shaping the sociotechnical infrastructure that constituted ERL. The rapid dissemination and shifting nature of school policies to enable ERL, however, created a breakdown because it required teachers, parents, and students to actively improvise in gray areas. This was particularly true when a policy could compromise privacy, such as policies regarding camera use.

While most participants mentioned that their school administration at the district and individual school levels had taken some steps to ensure the privacy and security of their students during ERL, the exact measures taken—and parent and teacher responses to those policies—varied. For some schools using Google as their main educational platform, participants described administrators enforcing settings like only allowing teachers to start/end video calls and requiring students to log in using their school account. Participants said that many schools also blocked certain websites (e.g. YouTube, social media websites) from being accessed on school-issued devices. Many schools had policies regarding camera use during synchronous learning (see Table 2), with some requiring cameras be on at all times. Schools also often dictated whether teachers recorded their Zoom classes and shared these recordings with students in ERL. All of these policies were developed quickly early on in the pandemic to enable ERL and schools updated them as the pandemic wore on.

When asked about the privacy and security measures taken to protect their children's data in ERL, some parents and teachers said they trusted the administration's policies and did not think about it further, while others highlighted challenges they faced with these ambiguous/shifting policies around data sharing, camera usage, and checking engagement and attendance. Some felt they had to place trust in the school system, including T5 (*"How did I manage [privacy and security]? I just trusted the county"*) and T10 (*"I just trusted that the school had it private."*) Other parents

and teachers were unhappy with their school or district administration's response to ERL privacy and security policies, sometimes describing them as too inflexible. For instance, P16 reflected, *"We honestly felt like there was too much security. The hurdles and the various clicks and things and the password protected log-ons. I thought that was overkill."* Similarly, P2 explained that their school had a policy where parents could sign a form to allow teachers to share photos of their child; with ERL, this included photos taken of children on video calls with anything in the child's background present in the photo. P2 explained that the policy implied the photos could either be shared in a small group of students/parents or publicly on the district website, bemoaning this lack of options, saying: *"It's almost an all-or-nothing where I wish there was more of an option. I'm comfortable sharing if it's only going to be seen by her class versus something that's going to be on the web for anybody to just kind of come across. So I wish there were more granular options."*

Interestingly, regardless of their views, neither parents nor teachers discussed having much interaction with their school or district administrations during ERL. In most cases, the school/district administration determined a policy for enabling ERL and safeguarding children's interests and then left parents and teachers to manage, work around, and negotiate that policy on an individual basis. Some teachers mentioned a lack of timely communication and consensus from school administrators, resulting in confusion and fluctuation between policies on virtual learning. T17 noted:

> *I think that with virtual learning, there were so many things that were violated. There wasn't a clear path for us to get usernames and accounts to students, there wasn't a clear way of oh, do we record, do we not—we started recording. So now those videos exist, [but] they shouldn't exist. There are so many hairy parts that just didn't have clear concise rules.*

This quote was typical of what we heard and demonstrates the rapid and reactive policies for everything from logging on to recording student data that were implemented, particularly earlier in the pandemic, and how they led to confusion and breakdowns in understanding for our participants. These breakdowns then created challenges for parents and teachers to keep learners engaged and online.

Numerous parents and teachers specifically brought up difficulties implementing or following policies regarding student camera use during synchronous online learning, noting that they needed to modify them because other parts of the sociotechnical infrastructure (e.g., wifi, multiple children on devices, etc.) were not capable of upholding the policies. T9's school, for example, had a "cameras-on" policy that meant students were marked absent if they did not turn their cameras on. T9 lamented the difficulty of enforcing this policy, as many students in their class continued to leave their cameras off in spite of the consequences. T9 partially attributed this to a lack of parental oversight and enforcement. P9, a parent who was also a high school teacher, described bandwidth issues created by cameras-on policies, particularly in households with multiple children on devices or without a strong Internet connection. In addition to practical considerations, some parents and teachers voiced misgivings regarding privacy concerns raised by strict cameras-on policies. P8 noted, *"My second grader is required to stay on the Zoom camera during school. And anyone who feels like looking at him within the house, of the other students in his class, they can see him, and if he's talking, they can hear him. Given a choice, I would not have picked that."*

4.1.3 Breakdowns in Authentication Infrastructure for Young Children. While many students struggled with authenticating into remote learning systems, our participants reported that the breakdowns in this infrastructure were particularly arduous for the youngest students. Parents and teachers explained that account management and access (i.e., getting students logged into accounts) were challenging processes for young children, who may still be learning their letters and likely had limited experience using a keyboard. Beyond that, most young children did not have email

accounts or had never had to set up and enter passwords prior to the pandemic; with the sudden shift to ERL, this created significant challenges in getting students online and accessing the correct content. P10 was surprised to learn their child, a first grader, had been given an email account: *"I was like, "My son has an email?" But they're not allowed to have access to it. You can't send anything to that email. I don't know at what age, I think sixth grade, it becomes an actual communication device. Right now it's just a log-in, a way for you to access a lot of sites."* On the other hand, teachers found these email accounts helpful since they typically required students to use district-provided credentials to log into synchronous video sessions which improved security (e.g., making it more difficult for an unwanted intruder to Zoombomb the classroom).

Beyond the challenge of setting up email accounts and using them to access school-related content, young children also struggled to remember passwords for remote learning. P5 shared an anecdote that highlights this challenge, describing the school district changing everyone's passwords with no notice. While annoying to the adults, this raised unique challenges for young children; as P5 noted, *"what kind of password do you expect a five-year-old to be able to easily remember and use on a regular basis?"* Another parent described being against the use of biometric passwords in general, but said they got so frustrated with their children's inability to remember their ERL passwords that they set up biometric passwords on devices the children used.

In summary, ERL exhibited infrastructural breakdowns that impacted privacy and security for elementary school children. In order to make ERL work, parents and teachers adopted a litany of technical tools that often felt overwhelming given that they needed to be learned from scratch and were largely not designed for an ERL context. For example, the video conferencing tool Zoom was originally designed for enterprise clients and the quiz platform Kahoot! was designed for use in a physical classroom. In cobbling together this patchwork of tools, parents and teachers did not have the capacity to prioritize digital privacy and security, and the tools themselves did not make information on these topics easy to access. Remote schooling was also largely influenced by district, school, and classroom policies that were often ambiguous and left gaps that teachers and parents needed to navigate because they conflicted with on-the-ground experience. For example, questions representative of our data are: how should teachers balance policies requiring students' cameras to be turned on with knowledge that some students faced bandwidth issues? How should they navigate policies saying online classes should be recorded with uncertainty on how to get informed consent from young children? Should such a policy require parent approval? Parents and teachers did not have the time needed to work around policies and craft guidelines, or deeply consider privacy and security, as their focus was on sustaining their children's online education. Lastly, as young children were forced to adopt adult technologies (e.g., Zoom), it became clear that they could not manage the largely password-based authentication processes these tools required.

4.2 RQ2: Privacy and Security Tensions Arose in ERL Around Public and Private Information And Spaces

Tensions unveil ways that the ongoing development of the ERL sociotechnical system stressed and shifted social norms around private/public information and home/school spaces. Many of the tools used during elementary school ERL made it easier to track and monitor students, teachers, and parents, and our participants were concerned about the impacts of this surveillance. That said, concerns related to these tools were in tension with learning goals, as parents and teachers described prioritizing the already-challenging task of getting children engaged in online school despite sacrificing privacy and security. We found surveillance tensions in ERL existed at two levels: (1) concern about teachers and parents monitoring students in new ways owing to ERL (4.2.1), and (2) unease about "bad actors" (e.g., hackers, technology corporations, or even school districts) using collected data to harm students (4.2.2). In addition to surveillance tensions, the blurring of

the boundaries between home and school in ERL created tensions around the respective roles of parents and teachers in children's lives (4.2.3).

4.2.1 Tensions Around Increased Monitoring in Synchronous Remote Learning. The tension between wanting to ensure children are safe and learning appropriately online and what constitutes too much surveillance was pushed to the forefront during ERL as digital tools allowed for easier monitoring of students. For example, teachers had access to a variety of tools (e.g., GoGuardian and Hāpara) that allowed them to see what students were doing on their screens at any given moment. Others noted these tools were already in use pre-pandemic, but that they became more critical with the shift to remote learning. For instance, participants spoke of how these tools helped with determining if a student was engaged during remote learning in the absence of more transparent forms of classroom monitoring (e.g., walking around the room, peering over shoulders) available in an in-person learning environment. If a student was, for example, playing an online game during a synchronous ERL lesson, teachers could observe this behavior and take action, including remotely exiting the game or even shutting down the student's computer.

Both teachers and parents felt student monitoring during online class time was appropriate; however, the forms these monitoring practices took during ERL were often deemed more invasive than those employed in the in-person classroom. Participants also spoke of how children felt they were being unfairly surveilled in these ERL instances; for example, T6 noted, *"The thing I heard from the kids was, 'It's my computer. You shouldn't be looking at what I'm doing online.' And I'm like, 'Woah, wait a minute. It's not your computer. It's a [school district] issued device."* This issue of ownership—students were using school-issued technology rather than personal devices even though they were physically at home—may have helped teachers rationalize student monitoring, with participants noting that this was similar to how they would manage what children were doing in a classroom.

In our interviews, parents discussed why they chose to monitor (or not) their children's online activities during the pandemic and ERL, including limiting screen time, blocking access to certain apps (e.g., Instagram, TikTok), and ensuring their children were communicating 'appropriately.' Some parents felt they should be able to check their child's accounts *"whenever I want"* (P3). Other parents resisted school surveillance by having their children log into remote schooling platforms using private—rather than school-issued—devices because they did not have tracking software.

Some parents qualified their opinions on monitoring children during ERL, saying they only wanted to control apps where there was a chance of harm (e.g., social media, gaming); educational or library apps were seen as low-risk. A few parents went so far as to describe tracking a child online as a breach of trust and, potentially, a security threat. For example, P2 described a school program that allowed parents to get notifications listing all of a child's online activities: *"I did not sign up for it, because I'm very much like, 'I don't want to know. I don't want to be seen like I'm spying.' And generally I am trusting of what he's doing, but that [program] definitely worries me a little bit, because I'm assuming the school also has access to all that data. What are they doing with that information?"* Still other parents avoided establishing explicit rules for their children in ERL, referencing their inability to definitively control or protect their children online. Moreover, some said that exerting such a level of control would compromise their children's ability to develop critical skills. As P12 noted, *"We can't strictly regulate all their devices in this environment, and I'm not confident I want to because we really want them to learn self-regulation."*

Parents in our study also discussed the increased burden of monitoring their children's participation in ERL. Though teachers generally established rules and expectations for synchronous instruction, parents said they ultimately had to enforce these rules. This required parents to keep an eye on both their children's screens to ensure ongoing engagement with school content, but

also on children's physical environments and activities. Some parents told us that maintaining an effective home learning space required managing children's interactions with nearby siblings and toys, compliance with camera and microphone protocols, and even physical attire and behavior. P12 described their experience with ERL, saying, *"I would come in sometimes and the camera would be off and the kid would be there in his underwear doing jumping jacks [in PE class]. I was just like, 'Oh God, I'm glad that you know to turn off your camera and you're not showing the world your underwear, but can we just put pants on please?"'*

For parents of younger children, there was an enhanced need to closely monitor their children's synchronous lessons, in part due to the level of adult support required for managing the technological and, at times, emotional demands of participation. P5, who had children in PreK and Grade 1, noted:

> *Her teacher wants [the camera] on, but at the beginning of the school year, my daughter would turn it off a lot. We transferred to a new school so these were kids she didn't know, and she also tends to have a little bit of beginning-of-school anxiety. And so, at the beginning of the year, it was hard to get her to keep it on. I was like, "If you can, please." And then there was one time where she got really upset, and I turned the camera off for her because I didn't think her classmates needed to see her upset.*

While this direct supervision of children's educational activities during ERL reflected parents' commitment to supporting their children's learning and protecting their privacy and safety, these interventions arguably represented a reduction in the level of autonomy and responsibility young students might otherwise experience in an in-person classroom setting. For example, many teachers described observing parents give their child answers to questions posed during synchronous instruction, posing obstacles to children's education and teachers' progress monitoring. Overall, ERL required parents and teachers to grapple with tension between the appropriate amount of monitoring needed for learning and harmful parent/teacher surveillance—a tension that was continuously negotiated but not resolved.

4.2.2 Tensions Around Increased Institutional Surveillance and "Big Data". Many teachers and parents felt uneasy and uncertain about the rise in large-scale collection of student data due to the increased use of digital tools in ERL. Participants had a sense that private information was being collected and could be used nefariously, but they were not sure what, if anything, they could do. The Family Educational Rights and Privacy Act (FERPA) [20] protects some student records at the federal level; however, no participants directly mentioned this legislation, and they seemed more concerned about student data that could be monetized by companies, sold to third parties, made inappropriately public, or stolen by attackers. T12 said they felt there was always some risk involved in sharing data online, noting, *"It's somewhat of a scary world that we're living in. I'd like to think we're protected on the backend even through Google Classroom and things that we're posting. But I'm sure that for the people who want to get in, those hackers... I know that that's a risk that we're taking."*

While T12 acknowledged risks to using technology in the classroom, they were unable to articulate who exactly would be hacking and what they would do with the data. Many teachers also told us how they were suddenly responsible for recording their synchronous lessons with children in ERL, which led to questions regarding how to best protect video data containing children's names, faces, and voices. Going back to T12, they discussed this unease around recording classes saying, *"After about two years, I will archive [the class recordings] and delete them. I'm always hesitant with the archive situation because that's not deleted. And then even when things are deleted, are they really deleted? I don't know."*

T12's questioning of their technical knowledge is unsurprising, especially when considering that many teachers had limited experience with many of the technologies for ERL before the start of pandemic. Other teachers also questioned data collection practices associated with the many different educational technologies used in ERL. For example, T9 noted that while they may not have known specifics, they were *"pretty sure the data just doesn't stop there [with instructors]."* Still others developed coping strategies for dealing with this uncertainty by coming up with schemes to anonymize children's data in ERL when possible. For example, T8 explained how they handled account setup in the Remind app (a communication tool): *"when we did Remind app, it was like, don't put student information, don't put names in, just put a parent's first name and last initial."*

For teachers who followed this or a similar approach, it was a simple method to limit student data being shared with corporations at a time when remote learning was needed. Importantly, the fact that individual teachers were concerned about student data collection and worried they were not savvy enough to manage this process suggests another component of the sociotechnical infrastructure of ERL: that when privacy and security is not managed by other parts of the system (e.g. by school administrations, government policies protecting student data, tools/educational resources to aid teachers with managing student data), this burden falls fully on teachers who likely have not been provided with the time and resources needed to feel like they can tackle it successfully.

While most parents did not express strong opinions or concerns about data collected as part of ERL, there were a few notable exceptions. P12 was among the most vocal, describing their anger at the district's implementation of a Chrome extension (without parent consent) to monitor students' browser-based activity from home. They explained, *"Basically this plugin... it allows them to see what your kid's doing on their Chrome browser. I get that they felt like they could do that because it's within district policy, it's within school hours, it's when kids are supposed to be in class, but I was super mad. So for a while, I forbid my kids to use the Chrome browser at all."* The absence of similar comments from other parents could likely be attributed to a number of factors—parents had many competing demands for their attention during ERL and privacy considerations were likely low on their list of priorities. Like teachers, parents may also have felt they lacked the knowledge and skills to assess whether these technologies were problematic, or they may have trusted that the district vetted all technology before it was used in the learning environments. This was the case for P14, who was fine with any tracking on school-issued devices, but said they would not have allowed school-mandated downloads on personal devices, if they had been required. Overall, ERL led to increased data collection about students, parents, and teachers by educational and non-educational technology vendors and it was not clear to the parents or teachers in our study how to assess the risks of this increased data collection on learners, families, or school practices.

4.2.3 Tensions Around School and Home Boundaries Blurring. During synchronous remote learning, tension developed between the newly blended home and school contexts and the appropriate role of parents and teachers in this hybrid interaction. For example, teachers were unsure to what extent they could—or should—interfere when students' homes were disruptive to learning. Multiple teachers described students who had distracting and non-private learning environments in ERL, including TV and music playing in the background, multiple siblings having lectures in the same space, or connecting to class while still in pajamas. T5 noted that these distractions meant that "*a lot of kids just weren't engaged.*"

While most of these distractions were relatively mundane, uncomfortable incidents at home that were broadcast into a ERL classroom stood out sharply for teachers—and for parents who witnessed these events. At times, teachers described these incidents as merely annoying, such as when a parent brushed their child's hair during class, children falling asleep, and parents walking

behind the screen without a shirt on. At other times, teachers shared more traumatic examples. For example, T6 remembered:

> *Literally the first day of school I had to call child protective services. The camera was off, but the mic was hot and [the student] was getting hit and yelled at by the father. I had to mute the student because at first I was kind of like, "No, this isn't what I think it is." And then we all kind of paused, the whole second grade class. I don't know if they knew what it was, but I knew what it was and I was like, "Oh my God." And so I just hit mute.*

T6 was not the only teacher who said they called child protective services during ERL. While this practice is not new—teachers have always been responsible for reporting threats to children's safety—ERL provided teachers with a more direct window into children's lives and added complexity to managing the classroom and looking out for their students. Beyond that, teachers described a lack of direction from administrators on how to proceed with this enhanced visibility into home life. They described developing strategies for managing different kinds of incidents in the home. For example, T10 described a challenging environment where they had to constantly monitor what was happening in the background while teaching *"to make sure that they weren't exposed to something that they shouldn't see or hear."* The blurring of home and school contexts is unique to virtual learning environments where synchronous meetings bring traditionally private spaces to the foreground. Synchronous context collapse created new challenges during ERL and teachers were inadvertently put on the front lines of managing it.

Additionally, teachers reported feeling like they were under greater scrutiny and more likely to be judged by parents—who might be watching their teaching over video calling platforms and be inclined to directly confront them during class in ERL. Several teachers mentioned parents cursed at them or were rude or aggressive during class in front of all of their students. T3 was concerned about parents being overly involved in ERL, saying, *"I think the most significant part of privacy and security is parents being completely all eyes and all ears, all the time. And it has nothing to do with having something to hide, but it has to do with the meddling where these aren't teaching professionals."* T3 also noted that parent criticism could be directed at students, as was the case with a parent who entered a class Google Meet session and began aggressively chastising one of their child's peers.

Overall, in this section we explored tensions that emerged in ERL between learning objectives and concerns over parent/teacher monitoring and institutional surveillance as well as the tensions between parents and teachers that resulted from the collision of the home and school contexts. These tensions illuminated how privacy and security were managed and negotiated in ERL due to the fact that ERL demanded parents and teachers actively consider what was"private-enough" or "secure-enough" in a crisis situation. While these tensions may have been particularly poignant during ERL, they remain as children continue to use online tools for learning.

5 DISCUSSION

In this paper, we examined teachers' and parents' experiences with ERL to better understand privacy and security issues impacting elementary school children. We did this by framing ERL as a sociotechnical system and identifying infrastructural breakdowns and tensions to explore how privacy and security were negotiated by parents and teachers during this time. Breakdowns we identified highlighted how privacy and security were deprioritized during the shift to ERL, both by teachers and parents who focused their time and energy on maintaining learning environments during a time of high uncertainty, and by administrators, who did not adjust policies to enhance children's privacy and security while learning from home. We also identified privacy and security tensions arising from the use of digital technologies to facilitate ERL and from the blurring of school and home contexts.

In this section, we detail three core ways our study can help researchers respond to privacy and security challenges raised by new technologies, particularly as they are appropriated during an emergency situation. First, we describe what we observed in ERL as a *contingent sociotechnical system*, a term to help the research community characterize the nature of these types of systems so we can better understand how they stretch privacy and security norms and boundaries in a time of crisis. Second, we argue for the adoption of *care* as a framework for designing future privacy and security infrastructure for children. Third, we detail specific design directions that emerged from our findings for improving privacy and security for children in digitally mediated learning environments.

5.1 Privacy and Security is Deprioritized in Contingent Sociotechnical Systems, Impacting Vulnerable Groups

We characterize ERL in the first year of the pandemic as a ***contingent sociotechnical system*** because it was ad hoc, precarious, and reliant on a complex web of adapted technologies and extraordinary efforts of stakeholders like parents and teachers. The Oxford English Dictionary defines *contingency* as *"the quality or condition of being subject to chance and change, or of being at the mercy of accidents."* Hence, we define a contingent sociotechnical system as an assemblage of technologies and social actors that exist in a particular unforeseen state due to a crisis or emergency event.

Our findings show that privacy and security were deprioritized during ERL, as parents and teachers worked on the more pressing goal of allowing children to continue their education remotely. While attending to privacy and security concerns may not seem like the most critical task in a moment of crisis, lack of attention in this area can cause long-lasting harm [45]. We argue that the deprioritization of privacy and security is a characteristic of the contingent sociotechnical system and that the most vulnerable groups, such as children, have the highest risk of harm. From our conversations with parents and teachers, it became clear they experienced significant stress and anxiety as they were forced to become front-line innovators, in charge of managing the education and well-being of children, while also juggling their own lives during the lockdown. In order to cope with this task in a crisis moment, they reached for any available tools that might help them with ERL, leading to a patchwork of technologies that parents, teachers, and children had to both learn and make use of at the same time. These off-the-shelf technologies were often ill-adapted for ERL, and privacy and security issues abounded. Moreover, institutions reacted to the rapid shift to ERL by implementing policies without taking time to evaluate whether they raised privacy/security risks, impacted student well-being, or were even practically achievable.

While we did not set out to explore differences across socio-demographic groups, it became evident while speaking with our participants that families with resources could opt out of some forms of surveillance if they chose, making children in resource-constrained families the most vulnerable to the deprioritization of privacy and security in the contingent sociotechnical system. Families who could afford to provide their children with their own laptop or tablet, for example, could limit surveillance built into school-issued devices. In contrast, our findings also highlight how families without these resources cannot opt out of these systems as easily. In contingent sociotechnical systems, where issues like privacy are not considered integral to the design of the system from the outset, there will be problems with equity and justice because those with the least resources will be most negatively impacted. This tension has been pointed out by data justice researchers in societal contexts outside of education [10, 17, 75]. As school and work activities move online, questions of who has the power to surveil and who can escape this will become an increasingly important topic for future studies. In the case of education, more research is needed

on what measures can ensure that technologies and the data they collect are not putting particular groups of children at risk.

Identifying social/technical assemblages as contingent sociotechnical systems that carry high privacy and security risks for vulnerable populations is useful for designers and researchers. In the case of ERL, it is clear that digital technologies continue to be integrated into classrooms and that the concerns we identified may be a harbinger of issues to come. The contingency of the ERL system should serve as a warning sign that we are far from being in a state where privacy and security issues are well-managed; thus, it is critical to address these issues now. In addition, fully remote learning will continue to play a part in education, both as a more accessible form of learning for some [69] as well as when necessitated by future crises (e.g., pandemics, global warming-related natural disasters, war). To avoid a state of contingency in future remote learning scenarios, we advocate for organizations to collectively tackle the issues that bubbled up during the pandemic *before* crisis hits.

5.2 Reframing Privacy and Security Work as Care Work in the Context of Education

One approach to privacy and security in computer science has been to treat it as a purely technical problem. Our findings, however, show that privacy and security tensions—such as how much student monitoring is acceptable or where the line between home and school exists—are often social in nature. Further, this technical orientation often occludes factors such as: the significant human labor needed to keep systems secure [33]; the fact that the boundaries between what is considered secure/insecure and private/public are culture-specific and constantly under negotiation [16, 30]; and the importance of trust/relationships in maintaining a sense of privacy and security for individuals, particularly those in vulnerable groups [77]. Recent work has built on feminist notions of care to reorient conceptions of privacy and security work towards understanding it as a relational, affective, and ongoing practice of *"collaborative tinkering and experimentation"* [33] (p. 92). The emphasis on care implies there are no magic fixes to privacy and security that solve these issues for good; instead, they require continuous attention and dedicated resources.

We argue that a care-based framework is a helpful lens for considering the privacy and security risks technology poses for children in educational settings. As Steeves and Jones [74] contend, *"to be a child is to be under surveillance"* (p. 1). If children, particularly young children in elementary school, have less autonomy than adults and are to some degree always under supervision, how should parents, teachers, and caregivers draw the line for how much surveillance is too much? What does it mean to protect the privacy of a young child? Here, the framework of care serves as a useful intervention: by shifting the question to ask how to best care for young children—thus centering their well-being—we can begin to grapple with what forms of monitoring are justified. It is important to note that this approach does not advocate for reducing children's autonomy; rather, a care-based approach should equip children where possible with the tools needed to manage their own digital lives.

Care as a framework for children's privacy and security in education also allows us to see this work as just one of many ways that children are cared for during the educational process. This acknowledges that there are competing care priorities and encourages honest conversations about how these competing priorities intersect. For example, educators must take into account the complexity of managing children's needs, which includes privacy and security needs (e.g., helping children to realize that they do have rights with respect to their data and to explore them in a meaningful way), logistical needs (e.g., getting kids to school and focused on lessons), and pedagogical needs (e.g., ensuring students are meeting educational milestones). We found that in a contingent sociotechnical system, tensions between these needs/priorities are exacerbated and strained. By folding privacy and security into a conversation about caring for children, it ceases

to be something "other" that is the responsibility of an "other" and is instead part of the work of those who care for children. This is not to say that teachers and parents should bear the full burden of protecting children online; institutions devoted to caring for children such as schools should consider this part of their responsibility and develop institutional privacy and security support.

It is not always clear when care crosses over into control. Our findings complement work by Lu et al. [46] that highlights this tension through teachers' use of the educational tool ClassDojo to manage behavioral data about students. In their study, they found teachers used the same tool to both enact care (i.e., checking in with a student who was struggling) as well as control (i.e., threatening to detract points from a misbehaving student). Similarly, we found the widespread use of tools like GoGuardian in the ERL contingent sociotechnical infrastructure allowed teachers to check student engagement and progress toward learning objectives, but that this, at times, felt invasive to students and parents. These systems can also be abused; for instance, a report revealed that in 2020, in one of the largest US school districts, teachers could initiate calls to student webcams through GoGuardian that were automatically answered, providing a window into students' homes without consent [27]. Future research is needed to explore the boundaries between privacy and security as care infrastructure that can empower children and enhance their autonomy versus as a mechanism for control and surveillance.

Given that privacy and security as care is a relational practice, in addition to designing and implementing automated systems, the work of performing privacy and security management includes having conversations to educate children about privacy and security concerns, developing policies around acceptable data use, and providing children with resources so they can have autonomy over their own decisions about privacy and security. To that end, next we explore several avenues for future work to improve privacy and security for children in school.

5.3 Future Directions for Rethinking Privacy and Security as Care Work

In this section, we explore what it might mean to tackle sociotechnical infrastructure challenges in children's privacy and security from a care perspective. We see both technical and social avenues for future work that need to be addressed in tandem to better protect children online. Our first finding on breakdowns highlights areas where the design of the system can be improved through repair. We showed that privacy and security slipped through the cracks of the contingent sociotechnical system as parents and teachers focused on knitting together a disparate set of tools to get children online for ERL. Even before the pandemic, teachers were using a wide range of educational technology and described uncertainty regarding how apps and tools were selected by school administrators [36]. Future design work should consider how privacy and security can be prioritized in an educational technology landscape that is diverse and fractured. For example, tools could be developed to help schools better screen educational apps for potential privacy and security risks and easily allow teachers to submit new apps to be assessed. Rather than adapting office tools designed for adults (e.g., Zoom) to the school context, distance learning tools could be designed specifically for school-aged children. Beyond that, automated tools that can scan the terms of use and privacy policies of school-required technologies and provide insight to parents and teachers on potential risks in plain language (something that researchers have been working on in other contexts, e.g., [59]) would be fruitful directions for future exploration.

We found that shifting school policies left gray areas and, at times, contradicted on-the-ground judgement of teachers and parents. To improve these policies at the classroom, school, and government level, all stakeholders (parents, teachers, students, administrators) should be engaged in developing and testing policies well before they are needed. Policies should speak to camera use, recording and archiving lessons, data use, and more. In particular, our findings suggest that teachers seeing child abuse in the home is not rare and must be directly addressed.

Future work should also investigate how to create new and secure ways for children to access systems that are better suited for their age while still maintaining their privacy. For example, within the contingent sociotechnical system, there was no infrastructure in place for young children to securely access video conferencing software and online educational websites. Children were forced to adopt email addresses and create passwords to log into these systems, leading to a host of issues such trouble remembering traditional passwords, concern over giving kindergartners email addresses, and worry about the security of biometric passwords. By understanding infrastructural breakdowns as both social and technical and centering student care, we are able to envision ways of improving the system along both axes.

The tensions we detail in our findings illuminate how social norms are shifting in the contingent sociotechnical system in ways that should be carefully considered in new designs. We found that new forms of monitoring parents, teachers, and students produced privacy and security concerns surrounding the impacts of this monitoring. Prior work on the surveillance of professional truck drivers found that increased monitoring aimed at improving rule compliance had negative unintended consequences (e.g., effort spent finding novel ways to subvert the system) and often failed to fix systemic issues (e.g., underpaid and overworked drivers) [40]. In the context of elementary education, increased monitoring will also have unintended consequences, and future work should consider alternative ways of accomplishing tasks such as performance evaluation. From a technical perspective, this could mean investigating forms of synchronous class participation that are meaningful but do not require always-on camera use or that help young children show their engagement without compromising their privacy. Blurred backgrounds in video calls are one example of a design intervention that addresses this issue, but some research suggests this has limited efficacy [58].

In addition to monitoring concerns, we found concerns over institutional surveillance focused on the large-scale collection of student data by for-profit companies. Future work should investigate how policies can protect children's data since companies do not have an incentive to do so. Researchers can provide policy recommendations and push regulators to limit the amount of data corporations making educational software can collect about children [14]. We also looked at how the boundaries between school and home blurred during ERL. The social norms that dictate how parents, teachers, and students should behave in home and school contexts have been developed over many years. The rapid introduction technologies like Zoom can disrupt social norms, often in uncomfortable ways [54]. Future work should evaluate how technologies can be designed in ways that foster respectful and caring norms.

In this paper, we adopted an infrastructural and care-based lens to consider privacy and security in ERL as a systemic, sociotechnical issue and center the needs of children. This systems-level perspective stands in comparison to prior work that often looked at how researchers could equip parents and teachers with tools to help them support children's online privacy and security (e.g., [9, 35, 49, 50]). Taking this approach reveals ways technology can be designed to support privacy and security infrastructure (e.g., creating digital tools to manage approved apps and technologies for school systems) and ways policies are needed to enforce privacy and security within these infrastructures. While acknowledging that the complexity of the situation, including the competing priorities of stakeholders, means there are no easy fixes, we offer this characterization as a way to think through how to make real and lasting progress towards enhancing the well-being of children.

5.4 Limitations

Our study focused on ERL under a narrow set of factors; specifically, we were interested in understanding experiences of ERL among US-based elementary school teachers and parents. This focus, combined with the challenges of collecting data from teachers and parents who were struggling

to manage remote learning during a global pandemic, meant our data collection spanned most of 2021, when factors were rapidly shifting from week to week. This also means that participants' experiences from early in the year and at the end of summer could have differed. We attempted to mitigate these changing conditions by focusing our data collection protocols on capturing the shift to ERL and the technological challenges that accompanied this shift, which all of our participants had experienced for well over half a year.

The challenges inherent to parents and teachers of younger children are likely different from those experienced by parents and teachers in middle and high school. Likewise, we did not capture the voice of children in this study because we were not permitted to work with children remotely during the pandemic by the IRBs at our institutions and pandemic-era school district policies restricting research with children. Future work should consider how children of all ages navigated the shift to ERL, as well as new threats they faced or concerns that arose when school moved online. In addition, future work could look at the potential impacts of specific technologies used in remote learning, which was outside the scope of this paper. Our teachers primarily came from the Mid-Atlantic region of the US and all worked at public schools, so these findings may not apply in other contexts. Finally, all but one of our teachers identified as female and this may have influenced our results, although we note that this is largely aligned with national demographic data: 97% of PreK/kindergarten and 82% of elementary school teachers in US public schools identify as female [19]. Future work could investigate a broader demographic of participants and confirm the findings at a larger scale using quantitative measures.

6 CONCLUSION

In this paper, we investigated privacy and security infrastructure—and the breakdowns and tensions that emerged from this infrastructure—during elementary school emergency remote learning (ERL) in the U.S. during the COVID-19 pandemic. While most children returned to in-person school by late 2021, their need for online privacy and security remains high given their continued use of numerous online tools, as well as the threat of future crises—from pandemics to climate disasters—that might necessitate a return to remote learning. Through interviews with elementary school parents and teachers, we described two main findings. First, we highlighted breakdowns in ERL sociotechnical infrastructure that contributed to privacy and security concerns. Second, we found new and exacerbated privacy and security related tensions in ERL related to surveillance and the collapse of the home and school contexts during synchronous remote schooling for children.

Based on these findings, we argue that privacy and security issues can be overlooked in contingent sociotechnical systems as parents and teachers struggle to achieve higher priority goals, such as getting children engaged in learning materials. Building on prior work in CSCW/HCI, we suggest that thinking about privacy and security in elementary education from the perspective of *care* can help guide future interventions to grapple with the competing care priorities of parents and teachers (e.g., helping children learn, keeping children's data private, protecting children from harmful online content). Ultimately, we bring to light privacy and security concerns young children faced during ERL using an infrastructural perspective with an eye towards advocating for systemic change to safeguard children's privacy and security online.

ACKNOWLEDGMENTS

We thank Cody Buntain, Salma Elsayed-Ali, Ruipu Hu, Sunyup Park, Yow-Ting Shiue, and the anonymous reviewers for their valuable feedback on this paper, as well as the teachers and parents who shared their time and experiences with us. This project was funded by the National Science Foundation under awards 1951688 and 1951311.

REFERENCES

[1] Stephen J Aguilar, Hernan Galperin, Clare Baek, and Eduardo Gonzalez. 2020. When school comes home: How low-income families are adapting to distance learning. EdArXiv. https://doi.org/10.35542/osf.io/su8wk

[2] Yunjo An, Regina Kaplan-Rakowski, Junhe Yang, Jenna Conan, Widad Kinard, and LeaAnne Daughrity. 2021. Examining K-12 teachers' feelings, experiences, and perspectives regarding online teaching during the early stage of the COVID-19 pandemic. *Educational Technology Research and Development* 69, 5 (Oct 2021), 2589–2613. https://doi.org/10.1007/s11423-021-10008-5

[3] Michael K. Barbour and Thomas C. Reeves. 2009. The reality of virtual schools: A review of the literature. *Computers & Education* 52, 2 (Feb 2009), 402–416. https://doi.org/10.1016/j.compedu.2008.09.009

[4] Elana Blinder, Jessica Vitak, Marshini Chetty, Tamara L. Clegg, and Kevin Song. 2021. *Challenges and Opportunities Using Technology in the Classroom: Results From Focus Groups With Elementary School Teachers.* [White paper]. https://spe4k.umd.edu/wp-content/uploads/2022/02/SPE4K-Teacher-Focus-Group-Report-Anonymized-January-2022.pdf

[5] Aras Bozkurt and Ramesh C Sharma. 2020. Emergency remote teaching in a time of global crisis due to CoronaVirus pandemic. *Asian Journal of Distance Education* 15, 1 (2020), i–vi.

[6] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101. https://doi.org/10.1191/1478088706qp063oa

[7] Virginia Braun and Victoria Clarke. 2019. Reflecting on reflexive thematic analysis. *Qualitative research in sport, exercise and health* 11, 4 (2019), 589–597. https://doi.org/10.1080/2159676X.2019.1628806

[8] Cathy S. Cavanaugh, Michael K. Barbour, and Tom Clark. 2009. Research and Practice in K-12 Online Learning: A Review of Open Access Literature. *International Review of Research in Open and Distributed Learning* 10, 1 (2009). https://doi.org/10.19173/irrodl.v10i1.607

[9] Yan-Ming Chiou, Tia Barnes, Shameeka M Jelenewicz, Chrystalla Mouza, and Chien-Chung Shen. 2021. Teacher Views on Storytelling-based Cybersecurity Education with Social Robots. In *Interaction Design and Children (IDC '21).* Association for Computing Machinery, New York, NY, USA, 508–512. https://doi.org/10.1145/3459990.3465199

[10] Sasha Costanza-Chock. 2020. *Design Justice: Community-Led Practices to Build the Worlds We Need.* The MIT Press, Cambridge, MA.

[11] Helen Crompton, Diane Burke, Katy Jordan, and Samuel W. G. Wilson. 2021. Learning with technology during emergencies: A systematic review of K-12 education. *British Journal of Educational Technology* 52, 4 (2021), 1554–1575. https://doi.org/10.1111/bjet.13114

[12] Bronwyn J. Cumbo, Tom Bartindale, and Dan Richardson. 2021. Exploring the Opportunities for Online Learning Platforms to Support the Emergency Home School Context. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21).* Association for Computing Machinery, New York, NY, USA, 1–11. https://doi.org/10.1145/3411764.3445044

[13] Norman Denzin. 2010. The fundamentals. *An Introduction to Triangulation, D. Rugg, editor. UNAIDS Monitoring and Evaluation Fundamentals, Geneva, Switzerland* (2010), 12.

[14] Caitlin Dewey. 2022. California's New Child Privacy Law Could Become National Standard. *Pew Research Center* (2022). https://pew.org/3FLHGpK

[15] Nana Diana, Suhendra Suhendra, and Yohannes Yohannes. 2020. Teachers' Difficulties in Implementing Distance Learning during Covid-19 Pandemic. In *2020 12th International Conference on Education Technology and Computers (ICETC'20).* Association for Computing Machinery, New York, NY, USA, 105–109. https://doi.org/10.1145/3436756.3437029

[16] Paul Dourish and Ken Anderson. 2006. Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. *Human–Computer Interaction* 21, 3 (Sep 2006), 319–342. https://doi.org/10.1207/s15327051hci2103_2

[17] Catherine D'Ignazio and Lauren F. Klein. 2020. *Data Feminism.* The MIT Press.

[18] Lee-Ann Ewing and Holly B. Cooper. 2021. Technology-enabled remote learning during Covid-19: perspectives of Australian teachers, students and parents. *Technology, Pedagogy and Education* 30, 1 (Jan 2021), 41–57. https://doi.org/10.1080/1475939X.2020.1868562

[19] National Center for Education Statistics. 2020. *Digest of Education Statistics, 2020.* https://nces.ed.gov/programs/digest/2020menu_tables.asp

[20] U.S. Government. 1974. Family Educational Rights and Privacy Act (FERPA). https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html. Accessed: 2022-07-14.

[21] Xinning Gui, Yao Li, and Yanlai Wu. 2021. Teacher-Guardian Collaboration for Emergency Remote Learning in the COVID-19 Crisis. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (Oct 2021), 399:1–399:26. https://doi.org/10.1145/3479543

[22] Lisa E. Gurley. 2018. Educators' Preparation to Teach, Perceived Teaching Presence, and Perceived Teaching Presence Behaviors in Blended and Online Learning Environments. *Online Learning* 22, 2 (Jun 2018), 197–220.

[23] Reza Hadi Mogavi, Yankun Zhao, Ehsan Ul Haq, Pan Hui, and Xiaojuan Ma. 2021. Student Barriers to Active Learning in Synchronous Online Classes: Characterization, Reflections, and Suggestions. In *Proceedings of the Eighth ACM Conference on Learning @ Scale (L@S '21)*. Association for Computing Machinery, New York, NY, USA, 101–115. https://doi.org/10.1145/3430895.3460126

[24] Charles B. Hodges, Stephanie Moore, Barbara B. Lockee, Torrey Trust, and Mark Aaron Bond. 2020. The Difference Between Emergency Remote Teaching and Online Learning. *Educause Review* (Mar 2020). https://er.educause.edu/articles/2020/3/the-difference-between-emergency-remote-teaching-and-online-learning Accessed: 6/30/2022.

[25] Juan Pablo Hourcade. 2015. *Child-computer interaction*. Self. http://homepage.cs.uiowa.edu/~hourcade/book/index.php

[26] Sarah E. Igo. 2018. *The Known Citizen: A History of Privacy in Modern America*. Harvard University Press, Cambridge, Massachusetts.

[27] Nader Issa. 2020. CPS teachers could look inside students' homes — without their knowledge — before fix. *Chicago Sun-Times* (Oct 2020). https://chicago.suntimes.com/education/2020/10/5/21497946/cps-public-schools-go-guardian-technology-privacy-remote-learning Accessed: 2022-07-14.

[28] Steven J. Jackson. 2014. Rethinking Repair. In *Media Technologies: Essays on Communication, Materiality, and Society*, Tarleton Gillespie, Pablo J. Boczkowski, and Kirsten A. Foot (Eds.). MIT Press.

[29] Rebecca Jeong and Sonia Chiasson. 2020. *'Lime', 'Open Lock', and 'Blocked': Children's Perception of Colors, Symbols, and Words in Cybersecurity Warnings*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376611

[30] Nicholas John, Sven Joeckel, Dmitry Epstein, and Leyla Dogruel. 2022. Privacy and distance learning in turbulent times: a comparison of German and Israeli schools during the beginning of the COVID-19 pandemic. *Learning, Media and Technology* (Jun 2022), 1–14. https://doi.org/10.1080/17439884.2022.2089682

[31] Elizabeth Kaziunas, Michael S. Klinkman, and Mark S. Ackerman. 2019. Precarious Interventions: Designing for Ecologies of Care. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov 2019), 113:1–113:27. https://doi.org/10.1145/3359215

[32] Alyson Klein. 2020. Cyberattacks Disrupt Learning Even More During COVID-19. *Education Week* (Sep 2020). https://www.edweek.org/technology/cyberattacks-disrupt-learning-even-more-during-covid-19/2020/09

[33] Laura Kocksch, Matthias Korn, Andreas Poller, and Susann Wagenknecht. 2018. Caring for IT Security: Accountabilities, Moralities, and Oscillations in IT Security Practices. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (Nov 2018), 92:1–92:20. https://doi.org/10.1145/3274361

[34] 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

[35] 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*. ACM, Trondheim, Norway, 67–79. https://doi.org/10.1145/3202185.3202735

[36] Priya C. Kumar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2019. Privacy and Security Considerations For Digital Technology Use in Elementary Schools. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, Glasgow, Scotland, 1–13. https://doi.org/10.1145/3290605.3300537

[37] Priya C. Kumar, Mega Subramaniam, Jessica Vitak, Tamara L. Clegg, and Marshini Chetty. 2020. Strengthening Children's Privacy Literacy through Contextual Integrity. *Media and Communication* 8, 44 (Nov 2020), 175–184. https://doi.org/10.17645/mac.v8i4.3236

[38] Priya C. Kumar, Jessica Vitak, Marshini Chetty, and Tamara L. Clegg. 2019. The Platformization of the Classroom: Teachers as Surveillant Consumers. *Surveillance & Society* 17, 1/2 (Mar 2019), 145–152. https://doi.org/10.24908/ss.v17i1/2.12926

[39] Katie Kyros. 2020. Zoom-bomber flashes 4th-graders; Baltimore City Schools tightens security. https://foxbaltimore.com/news/local/zoom-bomber-flashes-4th-graders-baltimore-city-schools-tightens-security

[40] Karen Levy. 2022. *Data Driven: Truckers, Technology, and the New Workplace Surveillance*. Princeton University Press.

[41] Na Li, Guillermo Romera Rodriguez, Yuqiao Xu, Parth Bhatt, Huy A. Nguyen, Alex Serpi, Chunhua Tsai, and John M. Carroll. 2022. Picturing One's Self: Camera Use in Zoom Classes during the COVID-19 Pandemic. In *Proceedings of the Ninth ACM Conference on Learning @ Scale (L@S '22)*. Association for Computing Machinery, New York, NY, USA, 151–162. https://doi.org/10.1145/3491140.3528284

[42] Xiaotian Vivian Li, Mary Beth Rosson, and Jenay Robert. 2022. A Scenario-based Exploration of Expected Usefulness, Privacy Concerns, and Adoption Likelihood of Learning Analytics. In *Proceedings of the Ninth ACM Conference on Learning @ Scale (L@S '22)*. Association for Computing Machinery, New York, NY, USA, 48–59. https://doi.org/10.1145/3491140.3528271

[43] Mark Lieberman. 2020. Massive Shift to Remote Learning Prompts Big Data Privacy Concerns. *Education Week* (Mar 2020). https://www.edweek.org/technology/massive-shift-to-remote-learning-prompts-big-data-privacy-concerns/2020/03

[44] Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri. 2019. *Children's data and privacy online: Growing up in a digital age. An evidence review.* London School of Economics and Political Science, London, UK. https://eprints.lse.ac.uk/101283/

[45] Bojana Lobe, Anca Velicu, Elisabeth Staksrud, Stephane Chaudron, and Di Gioia Rosanna. 2021. *How children (10-18) experienced online risks during the Covid-19 lockdown - Spring 2020: Key findings from surveying families in 11 European countries.* Number UR 30584 EN. Publications Office of the European Union, Luxembourg. https://doi.org/10.2760/562534

[46] Alex Jiahong Lu, Tawanna R. Dillahunt, Gabriela Marcu, and Mark S. Ackerman. 2021. Data Work in Education: Enacting and Negotiating Care and Control in Teachers' Use of Data-Driven Classroom Surveillance Technology. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (Oct 2021), 452:1–452:26. https://doi.org/10.1145/3479596

[47] 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)*. Association for Computing Machinery, New York, NY, USA, 1833–1845. https://doi.org/10.1145/2858036.2858251

[48] Sana Maqsood and Sonia Chiasson. 2021. Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens. *ACM Transactions on Privacy and Security* 24, 4 (Nov 2021), 1–37. https://doi.org/10.1145/3469821

[49] Sana Maqsood and Sonia Chiasson. 2021. "They think it's totally fine to talk to somebody on the internet they don't know": Teachers' perceptions and mitigation strategies of tweens' online risks. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Yokohama Japan, 1–17. https://doi.org/10.1145/3411764.3445224

[50] Sana Maqsood, Christine Mekhail, and Sonia Chiasson. 2018. A Day in the Life of Jos: A Web-Based Game to Increase Children's Digital Literacy. In *Proceedings of the 17th ACM Conference on Interaction Design and Children* (Trondheim, Norway) *(IDC '18)*. Association for Computing Machinery, New York, NY, USA, 241–252. https://doi.org/10.1145/3202185.3202753

[51] Annapaola Marconi, Gianluca Schiavo, Paolo Massa, Eleonora Mencarini, and Giulia Deppieri. 2021. From Sustainable Mobility to Good Deeds: Supporting School Participation during COVID-19 Emergency through a Playful Education Platform. In *Interaction Design and Children (IDC '21)*. Association for Computing Machinery, New York, NY, USA, 80–86. https://doi.org/10.1145/3459990.3460718

[52] Joseph Marks and Aaron Schaffer. 2022. Virtual learning compromised kids' privacy and security. *Washington Post* (2022). https://www.washingtonpost.com/politics/2022/05/25/virtual-learning-compromised-kids-privacy-security/

[53] David T. Marshall, David M. Shannon, and Savanna M. Love. 2020. How teachers experienced the COVID-19 transition to remote instruction. *Phi Delta Kappan* 102, 3 (Nov 2020), 46–50. https://doi.org/10.1177/0031721720970702

[54] Carolyn Marvin. 1988. *When Old Technologies Were New: Thinking About Electric Communication in the Late Nineteenth Century.* Oxford University Press, New York, NY.

[55] 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)*. Association for Computing Machinery, New York, NY, USA, 2273–2286. https://doi.org/10.1145/2998181.2998218

[56] Rebecca Michelson, Akeiylah DeWitt, Ria Nagar, Alexis Hiniker, Jason Yip, Sean A. Munson, and Julie A. Kientz. 2021. Parenting in a Pandemic: Juggling Multiple Roles and Managing Technology Use in Family Life During COVID-19 in the United States. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (Oct 2021), 402:1–402:39. https://doi.org/10.1145/3479546

[57] Ingrid Teixeira Monteiro, Marcelo Q. de Lima Brilhante, Jessica M. Ávila dos Santos, Francisco C. de Mattos Brito Oliveira, and Ana C. Bernardo de Oliveira. 2021. Mobile game-based learning with Opi app: Lessons learned with a children usability evaluation. In *Proceedings of the XX Brazilian Symposium on Human Factors in Computing Systems*. ACM, Virtual Event Brazil, 1–11. https://doi.org/10.1145/3472301.3484349

[58] Carman Neustaedter, Saul Greenberg, and Michael Boyle. 2006. Blur filtration fails to preserve privacy for home-based video conferencing. *ACM Transactions on Computer-Human Interaction* 13, 1 (Mar 2006), 1–36. https://doi.org/10.1145/1143518.1143519

[59] Razieh Nokhbeh Zaeem, Safa Anya, Alex Issa, Jake Nimergood, Isabelle Rogers, Vinay Shah, Ayush Srivastava, and K. Suzanne Barber. 2020. PrivacyCheck v2: A Tool That Recaps Privacy Policies for You. In *Proceedings of the 29th ACM International Conference on Information & Knowledge Management* (Virtual Event, Ireland) *(CIKM '20)*. Association for Computing Machinery, New York, NY, USA, 3441–3444. https://doi.org/10.1145/3340531.3417469

[60] 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

[61] Institute of Education Sciences. 2022. School pulse survey: School responses to COVID-19. (2022). https://ies.ed.gov/schoolsurvey/

[62] Trevor J. Pinch and Wiebe E. Bijker. 1984. The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology might Benefit Each Other. *Social Studies of Science* 14, 3 (Aug 1984), 399–441. https://doi.org/10.1177/030631284014003004

[63] Diyan Alfiyana Rahma, Retno Winarni, and Winarno. 2020. The challenges and readiness of elementary school teachers in facing society 5.0 through online learning during the covid-19 pandemic. In *Proceedings of the 4th International Conference on Learning Innovation and Quality Education*. ACM, Surakarta Indonesia, 1–6. https://doi.org/10.1145/3452144.3453743

[64] Prerna Ravi, Azra Ismail, and Neha Kumar. 2021. The Pandemic Shift to Remote Learning under Resource Constraints. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (Oct 2021), 314:1–314:28. https://doi.org/10.1145/3476055

[65] Farhad Saba. 2011. Distance Education in the United States: Past, Present, Future. *Educational Technology* 51, 6 (2011), 11–18. https://www.jstor.org/stable/44429966

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

[67] Katherine Schaeffer. 2021. What we know about online learning and the homework gap amid the pandemic. *Pew Research Center* (2021). https://www.pewresearch.org/fact-tank/2021/10/01/what-we-know-about-online-learning-and-the-homework-gap-amid-the-pandemic/

[68] Lorraine Sherry. 1995. Issues in Distance Learning. *International Journal of Educational Telecommunications* 1, 4 (1995), 337–365.

[69] Natasha Singer. 2021. Online schools are here to stay, even after the pandemic. *The New York Times* (2021). https://www.nytimes.com/2021/04/11/technology/remote-learning-online-school.html

[70] Svetlana Smirnova, Sonia Livingstone, and Mariya Stoilova. 2021. *Understanding of user needs and problems: a rapid evidence review of age assurance and parental controls.* London School of Economics and Political Science, London, UK. https://eprints.lse.ac.uk/112559/

[71] Kurt D Squire. 2022. From virtual to participatory learning with technology during COVID-19. *E-Learning and Digital Media* 19, 1 (Jan 2022), 55–77. https://doi.org/10.1177/20427530211022926

[72] Susan Leigh Star. 1999. The Ethnography of Infrastructure. *American Behavioral Scientist* 43, 3 (Nov 1999), 377–391. https://doi.org/10.1177/00027649921955326

[73] Luke Stark and Karen Levy. 2018. The surveillant consumer. *Media, Culture & Society* 40, 8 (Nov 2018), 1202–1220. https://doi.org/10.1177/0163443718781985

[74] Valerie Steeves and Owain Jones. 2010. Surveillance, Children and Childhood. *Surveillance & Society* 7, 3/4 (Jul 2010), 187–191. https://doi.org/10.24908/ss.v7i3/4.4151

[75] Linnet Taylor. 2017. What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society* 4, 2 (Dec 2017), 2053951717736335. https://doi.org/10.1177/2053951717736335

[76] Faiza Tazi, Sunny Shrestha, Dan Norton, Kathryn Walsh, and Sanchari Das. 2021. Parents, Educators, & Caregivers Cybersecurity & Privacy Concerns for Remote Learning During COVID-19. In *CHI Greece 2021: 1st International Conference of the ACM Greek SIGCHI Chapter*. ACM, Online (Athens, Greece), 1–5. https://doi.org/10.1145/3489410.3489426

[77] Emily Tseng, Mehrnaz Sabet, Rosanna Bellini, Harkiran Kaur Sodhi, Thomas Ristenpart, and Nicola Dell. 2022. Care Infrastructures for Digital Security in Intimate Partner Violence. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)*. Association for Computing Machinery, New York, NY, USA, 1–20. https://doi.org/10.1145/3491102.3502038

[78] Angel Walia and Grace Eden. 2021. The Worksheet School: COVID-19 Lockdown and Online Schooling in Public Schools of Delhi. In *India HCI 2021*. Association for Computing Machinery, New York, NY, USA, 140–144. https://doi.org/10.1145/3506469.3506493

[79] Ge Wang, Jun Zhao, Max Van Kleek, and Nigel Shadbolt. 2021. Protection or Punishment? Relating the Design Space of Parental Control Apps and Perceptions about Them to Support Parenting for Online Safety. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 343 (oct 2021), 26 pages. https://doi.org/10.1145/3476084

[80] G. Wang, J. Zhao, M. Van Kleek, and N. Shadbolt. 2023. 'Treat me as your friend, not a number in your database': co-designing with children to cope with datafication online. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3544548.3580933

[81] Zheng Yan, Yukang Xue, and Yaosheng Lou. 2021. Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers. *Computers in Human Behavior* 121 (Aug 2021), 106791. https://doi.org/10.1016/j.chb.2021.106791

[82] Jason C. Yip, Kiley Sobel, Xin Gao, Allison Marie Hishikawa, Alexis Lim, Laura Meng, Romaine Flor Ofiana, Justin Park, and Alexis Hiniker. 2019. Laughing is Scary, but Farting is Cute: A Conceptual Model of Children's Perspectives of Creepy Technologies. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, Glasgow Scotland Uk, 1–15. https://doi.org/10.1145/3290605.3300303

[83] Junnan Yu, Julisa Granados, Ronni Hayden, and Ricarose Roque. 2021. Parental Facilitation of Young Children's Technology-based Learning Experiences from Nondominant Groups During the COVID-19 Pandemic. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (Oct 2021), 1–27. https://doi.org/10.1145/3476048

[84] Leah Zhang-Kennedy, Christine Mekhail, Yomna Abdelaziz, and Sonia Chiasson. 2016. From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats. In *Proceedings of the The 15th International Conference on Interaction Design and Children* (Manchester, United Kingdom) *(IDC '16)*. Association for Computing Machinery, New York, NY, USA, 388–399. https://doi.org/10.1145/2930674.2930716

[85] Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. 2019. 'I make up a silly name': Understanding Children's Perception of Privacy Risks Online. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300336

7 APPENDIX

7.1 Additional Results from Teacher Demographic Survey

Our teacher demographic survey asked teachers to select all technologies they used as part of their teaching during emergency remote learning. Here we provide a list of our response options and the number of teacher participants who used each type of technology.

Table 3. Technologies Used by Teacher Participants During Emergency Remote Learning

Technology	**# Teachers**	**Technology**	**# Teachers**
Google Drive	14	PebbleGo	6
Google Meet	12	Go Guardian	5
YouTube	12	Kahoot!	5
Zoom	10	Screencasting App	5
ClassDojo	7	i-Ready Math	5
Starfall	7	Remind	4
ABCya!	6	Powtoons	3
Brainpop	6	iMovie	3
Course Management System	6	Seesaw	3
Flipgrid	6		

Received July 2022; revised January 2023; accepted March 2023