"I'm going to trust this until it burns me" Parents' Privacy Concerns and Delegation of Trust in K-8 Educational Technology

Victoria Zhong, *New York University;* Susan McGregor, *Columbia University;*
Rachel Greenstadt, *New York University*

https://www.usenix.org/conference/usenixsecurity23/presentation/zhong

This paper is included in the Proceedings of the
32nd USENIX Security Symposium.

August 9–11, 2023 • Anaheim, CA, USA

978-1-939133-37-3

Open access to the Proceedings of the
32nd USENIX Security Symposium
is sponsored by USENIX.

"I'm going to trust this until it burns me" Parents' Privacy Concerns and Delegation of Trust in K-8 Educational Technology

Victoria Zhong
New York University

Susan McGregor
Columbia University

Rachel Greenstadt
New York University

Abstract

After COVID-19 restrictions forced an almost overnight transition to distance learning for students of all ages, education software became a target for data breaches, with incidents like the Illuminate data breach affecting millions of students nationwide and over 820,000 current and former students in New York City (NYC) alone. Despite a general return to in-person schooling, some schools continue to rely on remote-learning technologies, with NYC even using remote learning during weather-related closures or "snow days." Given the ongoing use of these classroom technologies, we sought to understand parents' awareness of their security and privacy risks. We also wanted to know what concerns parents had around their childrens' use of these tools, and what informed these concerns. To answer these questions, we interviewed 18 NYC parents with children in grades K-8. We found that though the COVID-19 pandemic was the first exposure to remote learning technologies for many children and some parents, there was insufficient guidance and training around them provided for children, parents, and educators. We also found that participating parents implicitly trusted schools and the Department of Education (DOE) to keep their children - and their children's data - safe, and therefore rarely reported privacy and security concerns about classroom technologies. At the same time, however, they described many situations that indicated privacy and security risks with respect to classroom technologies.

1 Introduction

Although software has been widely used in primary, secondary and higher educational settings for well over a decade [73], its associated privacy and security risks were understudied until the COVID-19 pandemic. Like all software, however, software used in education carries privacy and security risks; according to one industry analysis, 44% of organizations targeted by ransomware in 2020 were in the education sector, another identified, 26 colleges and universities that had suffered cyberattacks in 2021 [12, 26].

A number of U.S. K-12 educational districts—some of which serve many times the number of students as a given college or university—have also been targeted for cyberattacks.In January 2022, for example, NYC's Department of Education (DOE)—which manages the largest K-12 school district in the US—acknowledged a data breach targeting third-party software provider Illuminate, which affected the data of at least 820,000 current and former DOE students, as well as hundreds of thousands more across New York State. According to the DOE, the breach exposed a raft of potentially sensitive data, including students' names, birthdays, student identification numbers (known as OSIS numbers), gender, ethnicities, home language, 'English Learner' status, course information, and economic status, along with whether they had received special education services[1] [55]. A number of other school districts across the country were also impacted by the breach [42].

The increased reliance on technology for teaching at all levels that began with the COVID-19 pandemic sparked new interest in the strengths and weaknesses of these tools, especially as students were mandated to use certain applications—some of which were not originally designed for use in the educational context, or by minors. As a result, though the mandated use of remote learning software may have reduced learning loss during the pandemic, it also introduced novel privacy and security risks. Our goal in this paper was to investigate those risks, especially for students under the age of 13, whose privacy and security are recognized as uniquely important under the Children's Online Privacy Protection Act (COPPA) [8].

Despite a general return to in-person teaching and learning, many of the technologies introduced during the pandemic continue to be used by school systems. In New York City, weather-related school closures or "snow days", for example, have been replaced by remote learning days [49]. Privacy and security risks in these technologies can be used to steal

[1]The precise details of students' Individualized Education Programs (IEPs), were not exposed [56].

childrens' identities; in 2011, for example, a representative study by Carnegie Mellon found that children under the age of 18 were 51 times more likely than adults to have their identities stolen [61]. Beyond this, critics posit that overreliance on these technologies may harm social and educational outcomes by normalizing a culture of surveillance, increasing students' self-censorship, and reducing educational equity [13, 25, 43, 47].

Because of these risks and the relationship between parental media use and that of their school-aged children [44], we sought to understand the security and privacy perceptions of parents with K-8 students regarding technology their children used in school. We wanted to understand whether parents understood what data was collected and retained, how data was handled and processed, and their knowledge and perception of security incidents. After learning of the Illuminate data breach, we also wanted to know whether parents were generally aware that this specific breach had occurred and their attitudes and concerns towards breaches.

Through semi-structured interviews with 18 parents of NYC public school children in grades K-8, our research provides a deeper understanding of parents' concerns around classroom technology use and what contributes to or mitigates these concerns. We chose to focus on parents with K-8 children in NYC's public school system, because it served over one million students in the 2020-21 school year [3], and is the largest school system in the United States. As such, the NYC district represents a large number of families dealing with uniform requirements to continue using remote learning tools even as students are meant to benefit from COPPA protections. We found that while many participants people did not report privacy concerns around classroom technologies, this was due in part to the implicit trust they placed in schools to protect their childrens' overall safety and well-being. As a result, we also sought to understand the role that institutional trust played in participants' privacy and security perceptions around classroom technology. Our study addresses the following research questions:

RQ1: What are the privacy and security concerns of parents with children in public K-8 programs with respect to classroom technology use, and what informed those concerns?

RQ2: How did trust in their childrens' schools and the NYC Department of Education influence their privacy and security concerns - or lack thereof - around classroom technologies?

Our interviews revealed the following:

1. The move to remote learning due to COVID-19 was one of the first—if not *the* first—experiences using technologies like email, video conferencing tools, Google Classrooms or even the internet for many participants' children, and some participants themselves.

2. There was an overall lack of guidance and training for parents, children, and educators on how to use this technology.

3. Parents felt uncertain about the risks of using the technology as well as how to combat them.

We also found that participants' privacy and security concerns were often *mitigated* by several factors:

1. The belief that the information collected about their children was harmless.

2. A desire for schools to monitor their children.

3. Participants delegated trust to schools and the DOE.

In particular, participants expressed that it was the school's responsibility to keep their children safe, and so trusted that the DOE's decision to adopt certain applications meant that they were "safe."

Based on these findings, we recommend that educators provide information about any new technology used to parents upfront and get expressed consent before signing students up for services and have alternatives available should parents opt out of services. We also encourage the security community to conduct independent audits of these technologies and provide guidance to educational leaders so that they can make better choices to keep students and their information safe.

2 Background and Related Work

To better situate our work, in this section, we review related work on children's privacy and security, and technology in the classroom more generally. We also briefly touch on special legal protections in the US for children under the age of 13.

2.1 Privacy and Security Risks Online

Recent work on children's privacy and security awareness indicates that they are generally aware of threats online [79, 80], and that they perceive privacy as a barrier to protect them from being watched or intruded upon [58]. Generally, children associate privacy and security threats with physical harm, or harm to their online accounts [69]. The most commonly identified threats were inappropriate content, strangers, oversharing, and getting "hacked", as well as cyberbullying and parental surveillance [69, 79, 80]. However, children were often less aware of data collection and tracking as a privacy concern [68, 69, 76, 80]. Indeed, some work suggests that children and teens see privacy through a lens of safety and identity management, and are either unaware of or overlook the potential risks of data collection [45].

For example, while children demonstrate some understanding that data collection can be used to make inferences about them, they often believed that their data was used mostly for improving services and ensuring safety, and that it would

remain solely on the device or platform where it was collected [69, 76]. Additional misconceptions include believing that monitoring is done by humans in real-time—and that therefore it was infeasible to monitor all users simultaneously [69, 76].

Parents' privacy and security concerns, meanwhile, centered around screentime, inappropriate content, childrens' self-disclosure, and "stranger danger" [79]. The "hacking" of smart home devices was also a significant concern as vector for strangers to reach their children [70]. At the same time, parents did not mention data collection by companies as a threat [70, 79].

2.2 Privacy and Security Strategies

While children often attempt to protect their privacy by withholding information and avoiding talking to those they don't know [45, 69], some children believed they could stop further data collection or delete information applications had on them by closing or deleting an application [69]. When faced with threats, children would often ask for help from parents [79, 80].

Parental strategies for mitigating online privacy and security threats to their children often involve monitoring children's activity and restricting access when necessary [70, 79, 80], yet there are indications that such restrictive methods may *not* reduce online risks, and can even increase harm for some children [22], perhaps by inhibiting their ability to learn how to protect themselves from these risks [77, 78]. Indeed, studies show that the best approach is not to block all exposure to online risks, but rather allow them some exposure to risk and use this exposure to teach and empower their children to develop strategies to cope with such risk [22, 77, 78].

While there is a lot of work on how children perceive and cope with online privacy risks, much work centered around parents, who facilitate children's technology usage focuses specifically on how strategies parents use to prevent risks, but not what factors inform parental concerns. Moreover, these works are in the context of voluntary technology usage where children have the ability to choose whether to interact with the technology, whereas any technology used in the educational setting is often mandatory.

2.3 Harms of Technology in the Classroom

Many works identified the potential harms that can occur due to technology in classrooms. While surveillance of children and students was practiced before the adoption of technology, technology allows surveillance to be much more pervasive. Alongside traditional surveillance, as schools begin to adopt data-driven educational technology, these too become a form of surveillance. Much like traditional forms of surveillance, surveillance through these platforms encourages conforming to normative thoughts and behaviors and discourages the exploration of ideas that may not fit the norm [48]—counterintuitive to the goals of education. More pressingly, these norms are subject to teachers' biases which may be informed by stereotypes of how a certain group acts. As such teachers may be more vigilant of stereotyped groups leading to marginalized groups being disproportionately surveilled and penalized as well as reinforcing existing prejudices [47, 63]. Moreover, as information generated by these platforms may be seen as impartial and objective truth, when a student's information is passed to future teachers, that teacher may create some bias affecting how that teacher evaluates the student [47].

This is especially true of gamified platforms such as ClassDojo where teachers can reward desired behaviors or punish students for undesired behaviors in real-time through the use of a point system. This classification of good vs bad behaviors is also divorced from context and thus fails to take into account the cause of students' behavior. As such, these students may be placed under increasing scrutiny rather than getting the support they need. This, however, does not only affect students who exhibit undesired behaviors. Indeed, Lu et al. due to lack of nuance, teachers may be misled into believing students who do not exhibit "bad" behaviors are not in need of support [47].

Moreover, school surveillance is not limited to just what students do in school or on school devices, as some schools turn to third party surveillance software to monitor students' social media accounts [64]. The behavioral and psychological effects of exposure to pervasive surveillance at a young age has been well documented [41, 47, 48, 63, 74], however, the amount of data collected raises additional privacy and security concerns [41]. In addition to unclear terms of data retention, it is also unclear what data third party monitoring software contracted by schools can access and how that data is used [64].

However, school surveillance does not only affect students, but teachers who are often the facilitators of surveillance. In order to provide students with support, teachers have to perform extra labor to contextualize students' behaviors. Moreover, as some of these platforms allow other stakeholders, *i.e.* parents, administration and even students, to themselves surveil teachers' surveillance, teachers are put under more scrutiny to document students' behaviors in a way that conforms with stakeholder expectations, thus creating a tension between providing care for students and performing to navigate stakeholder demands. Some teachers even felt the need to under-report students' negative behaviors to avoid the ire of parents or over-report them in order to get schools to provide more resources for their classrooms [46]. Thus teachers are subject to the same control enacted onto students.

Adoption of technology in an educational context also serves as an avenue to advertise to children, reinforcing and normalizing surveillance capitalism at a young age [14, 17, 72]. Boninger and Molnar identify schools as a lucrative target

for data collection due to their readiness to adopt technology especially if offered for no cost [17]. Though pervasive data collection is thought to be anonymous because it is collected in aggregate and de-identified, studies have shown that if improperly anonymized, data could easily be re-identified [16,54,60,71]. More pressingly, Gebhart et al. found that both parents and students were unaware of what data applications in schools collected and that often parents and users had to seek out privacy implications themselves [27].

There have been initiatives to evaluate potential privacy concerns with the use of applications for educational purposes. One such initiative was the *Common Sense Privacy Program* created by Kelly et al that sought to audit applications aimed at children so that parents and educators can make more informed choices about applications used by children [37]. Their platform details how privacy-preserving applications that are used in schools, and supplementary applications parents may choose to use for their children are, as privacy policies are known to be difficult and time consuming to read [50].

In a recent paper from Cohney et al, researchers modeled the risks of platforms used in the classroom e.g. Slack, Zoom, and Blackboard, and identified a conflict between almost all stakeholders. One major finding was that the companies who owned these platforms' data collection policies were in conflict with both educators and students. They also found that some platforms by default had the ability to harvest student data as well as distribute said data to undisclosed third parties [19]. The implications of this work show that without official institutional procurement that comes with stipulations on how data is to be managed, student data can be disseminated potentially anywhere. While Cohney et al.'s research focused on applications used in higher learning, some of these applications i.e. Zoom, Google Meets, are also used by K-12 schools introducing a new concern regarding minors' data potentially sold or distributed if used with its default settings.

2.4 Legal Protections

Though laws like the Family Educational and Privacy Rights Act (FERPA) and COPPA exist to protect students data, there is a mismatch between the expectations of the degree of protection and how much privacy protection is actually provided. Under FERPA, companies can be elevated to the status of school officials and are thus allowed to share student data with these companies without parental consent [17]. In the case of COPPA, though §312.4 states that sites must provide notice to obtain consent and inform parents of their rights to review or remove their children's data, studies have shown that people often do not read privacy policies before accepting them [32] and can be obfuscated either intentionally or by using language their audience do not understand diminishing the impact that the prohibition of mandatory collection of data has, as many parents may not know they can opt out of sharing certain data. [31].

Moreover as noted by Wang, because schools can used as intermediaries between parent and companies by the company, this shifts the responsibility of garnering "verifiable parental consent" as well as general compliance from the companies to schools [75]. In fact, schools can consent and even release students' PII *without* parental consent due to COPPA's inapplicability in schools so long as the data is educationally useful and not for commercial usage. Skowronski notes that limiting data collection to the educational context is ineffective because many websites and applications used for school are often embedded with third party trackers and are often not designed specifically for the educational context [67]. Thus, if a student moves from an educational application to a commercial application of the same company they would be subject to tracking [17, 67].

While companies have a duty to comply with these laws, the burden is placed upon students or parents of students to file a complaint if they believe their privacy has been violated. This requires parents to know not only that they can file a complaint, but how to do so [7]. Moreover in the case of COPPA, as Boninger states in the event that a complaint is filed, the FTC is unlikely to pursue the complaint [17]. Additionally, enforcement of these laws is often in the form of financial disincentives i.e fines or loss of funding, as such while this may be a deterrent for smaller companies, larger companies are unlikely to be affected as illustrated by Google's multiple and continued privacy violations [40, 52, 66].

3 Methodology

We conducted semi-structured interviews that lasted approximately 30 to 45 minutes with 18 participants.

3.1 Human Subjects Protection

Our institutional review board (IRB) has reviewed and approved our study protocol, interview materials, consent, and recruitment procedures. Prior to the interview, we provided all participants with a consent notice via email, and during the interview, participants reconfirmed their consent to the interview, recording, and retention of their emails for further contact. Interview participants were compensated with a $25 Amazon gift card after completing the interview.

3.2 Interview Design

The goal of our study was to elicit both the implicit and explicit security and privacy concerns of parents with respect to classroom technologies. Our full interview protocol can be found in A, though due to the semi-structured nature of our protocol, we did not explicitly ask every question of every participant, instead monitoring responses to ensure that all topics were covered in a given interview.

We began by asking participants what devices their children used for remote learning, and whether they were personal devices or provided by the DOE. We also sought to identify any "workarounds" parents or their children used to complete required tasks, as these can both create privacy/security risks and provide valuable insights for designing usable security approaches [38, 39] We also asked if alternatives were available for students uncomfortable with or unable to use a given technology, such as alternate applications or paper options.

We then asked whether participants knew if the schools monitored students' accounts and devices, and whether they would be comfortable with this. We also asked what access the teachers or administrators had to these accounts and devices.

We then asked whether classes were recorded and if having cameras on was required. We also asked about participants' comfort level around camera usage and recordings. Taken together, these first sections of the interview helped contextualize the setting in which students were doing remote learning and to indirectly gauge participants' privacy perceptions and concerns.

In the next portion of the interview, we focused specifically on privacy, though we intentionally declined to *define* privacy in order to better elicit how participants viewed privacy and what it meant to them. Though some participants wanted to know what specific aspect of privacy we were asking about, we encouraged them to rely on whatever aspects of privacy were significant to them. We then followed up with questions about their perceptions in the context of more specific elements of privacy *i.e.* data collection, data access, etc. We also asked participants about any privacy-related incidents. After our second interview participant mentioned the Illuminate data breach, we specifically asked subsequent participants about data breaches, though we did not mention Illuminate by name. As such, only the first participant was not asked about data breaches. We also asked about privacy concerns around general technology use, such as everyday web surfing, social media use, and device access to explore possible relationships between these concerns—or lack thereof—with regards to the use of technology usage in their child's classroom **RQ1**.

Lastly, we then asked about parents' trust in their institution, what would increase and what would decrease trust. We also wanted to know what parents would do should their trust in their child's school be eroded **RQ2**.

3.3 Recruitment and Demographics

We focused most of our recruitment efforts on parent organizations; all NYC public schools are required to have a Parent or Parent-Teacher Association that communicates regularly with all people in parental relation to enrolled students [11]. We specifically recruited for NYC parents aged 18 or older who had at least one (1) child enrolled in school in grades K-8.

We filtered the NYC DOE-provided list of public schools from NYC Open Data [57] for elementary and middle schools, then reviewed the related website for parent organization contact information. In lieu of this, we then looked for contact information for the school's parent coordinator.

Of 1193 elementary and middle schools, 1088 (91%) had a website. However, only 544 referenced a functioning parent organization page; in total we were able to directly contact 424 schools via email and requested they distribute our call for participants and signup link to their contact lists.

Participants scheduled their interviews through Calendly [1] and were interviewed on a rolling basis. Of 24 participants who scheduled an interview, 18 showed up.

Participant demographics Because of the qualitative nature of this research, we requested only enough demographic information about participants to confirm eligibility. All the interviewees were between the ages of 31 and 55, with the median age being 44. Our participants' children's grade level during the pandemic ranged from kindergarten to 8th grade, with the median being 4th grade. These interviews took place between May and July of 2022, approximately nine months after NYC had resumed in-person classes [62].

3.4 Interview Analysis

Interviews were recorded and transcribed by Zoom's live transcription feature; These transcriptions were afterwards edited for accuracy by the first author. The interviews were iteratively open-coded by the first author on a rolling basis by reading through the transcript, identifying discrete chunks that reflected distinct beliefs and ideas, and applying descriptive codes. Any time a new code was generated, prior transcripts were reviewed to see whether it applied to those results. This process of interviewing, transcribing, and iteratively coding was repeated until two consecutive interviews did not generate any new codes; we then determined that saturation had been reached. At this point, we coded one remaining interview that had already been scheduled; it also produced no new information. From there, axial coding was used to distill codes into categories and map relations among them. The first author identified articulated concerns, events or conditions related to concerns, actions taken in response to concerns or events, and rationales that contributed to or mitigated concerns. These axial codes were then applied to all transcripts.

Throughout this process, the authors met on a biweekly basis to discuss and refine the codes and reach a consensus about the categories and relationships of the axial codes.

3.5 Limitations

Due to the qualitative nature of this work, our findings cannot be generalized. Like other qualitative research, however, our findings help describe and make sense of reality and may support the development of explanatory models and theories [53],

though with the potential to support future quantitative research [29]. As with all open-ended interview studies, participant responses may not be comprehensive; thus while a given participant may not have expressed a certain concern or belief, this does not mean they did not have these concerns or beliefs. Additionally, our participants were self-selected and considered themselves to be both very active in their children's education, and very knowledgeable about what was happening in their schools, thus their experiences are unlikely to reflect those of all parents, even within similarly-situated NYC public schools. Likewise, while do not know how many schools are part of our participant sample, participants occasionally referenced their school by name during interviews, so we know at least 3 different schools were represented.

Finally, this work focuses only on the perspectives of parents. While we believe that the perspectives, concerns and limitations faced by educators and school administrators are key to a more complete understanding of the security and privacy risks of classroom technology use, we leave this investigation to future work.

4 Results

4.1 Background Information

All but four (4) participants used a school-issued iPad. The parents who chose not to use a school issue devices largely did so because they had their own devices and felt someone else could better make use of the iPad. Some of the iPads were reported to be able to connect to the DOE's Wide Area Network (WAN). All but one parent reported that their schools continued to use technology even after the lockdowns ended.

Participants reported that while there was a list of approved applications schools could use, it was largely up to the school and at times teachers to choose which applications to use out of the list and how to implement them in lessons. Most participants reported their children as having used either Zoom or Google Meets, iReady, and Raz-Kids. Parents reported that accounts were created for their children by the schools. Parents were unable to opt-out of the use of any of the applications the schools chose to use unless they voiced legitimate concerns, or did not have access to a device or internet—the latter of which is rendered moot because the DOE would provide both. It is unclear what counts as a legitimate concern as the parents interviewed did not attempt to opt-out. Paper packets were available in some schools, in some cases only for those without access to the internet or devices. However the participants to whom it was available to found it too inconvenient to use as they would have to pick up and return them in-person for accountability purposes.

4.2 General Security Concerns

Parents' concerns fell into five categories: (1) screentime, (2) exposure to inappropriate content, (3) strangers, (4) cyberbullying and (5) unauthorized parties gaining access to their children's information especially if their child had an IEP.

4.2.1 Screentime

Participants most explicitly expressed that they were concerned their children were having too much screentime. This was an issue parents had both with the use of technology in general and in an educational context. Parents were worried that excessive screentime would result in their children being dependant on or addicted to technology and could hinder children's ability to perform analog tasks such as writing, as well as their social and emotional growth.

> *The little ones didn't even know how to write their name pre-kindergarten...now it's all technology* - I2

4.2.2 Inappropriate Content

Almost every participant expressed some concern about their child being exposed to inappropriate content. While most of these concerns were explicitly expressed while talking about technology use in general, parents were worried about the potential for inappropriate content to appear even in an educational context.

For example, one parent described the vandalism of a teacher's webpage (detailed further in 4.3.3):

> *I would not want any of my kids to be exposed to the things that was placed online at my school...[it was] really very, very inappropriate on many levels - not just for a kid seeing it.* - I1

This concern manifested in a desire for educators to place controls on children's apps and devices. As one parent put it:

> *I've heard stories about like nine-year-olds finding porn on the Internet...If the iPad wasn't so restrictive I don't even know if I let them use it* - I7

4.2.3 Strangers and Creeps

The threat of "strangers" or "creeps" was also frequently mentioned as a threat when it came to their children's usage of technology in general, including educational apps:

> *What I didn't like about Adventure Academy is that anyone can be chatting...My kids at the time that they were using it were only six years old and some of his seventh year. That's way too young for anybody to be texting them* - I17

Participants with this concern stated that they would check who their children was communicating with and disallow contact with individuals they did not know, but as a result were generally concerned about their children being visible on-screen:

> *I don't know who's the one jumping into the call...[so I don't want] my child [to] show their face. I don't know who the other person on the other side of the screen is.* - I2

4.2.4 Cyberbullying

While no participant reported their child being cyberbullied, a few participants were worried their child might be cyberbullied by their peers. This concern was mostly in the context of the general usage of technology, however, two participants mentioned that they were worried that their children might be cyberbullied in the classroom. One parent pointed to the chat feature in virtual classrooms as a vector for cyberbullying, the other (I16) pointed towards the potential that students might use their smartphones to take pictures of other students during in-person classes and that they "*don't trust kids being appropriate with their cellphones as they got older*"

4.2.5 Loss of Information Control

Participants expressed that information collected about their children should stay within the school or district. In general, there was a belief that the data collected should be used for education. It had to directly benefit parents or their children, or aid educators in their ability to educate.

IEPs: Participants with a child or children with IEPs, a plan which laid out what accommodations students needed, were especially aware of the security risk this information could pose:

> *[IEPs] could be very, very detailed...People don't really understand that.* - I1

As a result, these parents worried about not only who had access to their child's IEP, but even who could discover their child *had* an IEP. Parents felt that only those who were involved in their children's education should have access to this information.

For other parents, the sheer number of individuals with access to their child's data felt like a privacy compromise:

> *Because of what's included in the IEP, I feel that [the schools] have a lot of information about us, more than a student in General Ed...I know [the IEP] gets transferred from teacher to teacher, I know it gets transferred from grade to grade and then, of course, if they're going from school to school.* -I4 [...]

Improper Disclosure: Some participants were concerned about data being collected and shared by educational applications. One parent (I1) questioned:

> *Who are they, who are iReady sharing stuff with?*

Some participants were also specifically concerned about the commodification of their children's data:

> *It wasn't like it was a DOE program, it was outsourced to Google. [My child's] information can be sold and purchased now .* -I3

As another put it:

> *Whatever data [app makers] get, I feel they use it to go ahead and try to sell a product, whether it be to us directly or to the DOE* -I4

However, technology was not the only means by which dchildren's information could be disclosed. Parents were worried that educators might be indiscreet when mentioning things pertaining to their child's performance.

> *I tell the teachers: make sure when you're discussing like her grades with me, it's outside...I wait for all the parents to leave because you know [teachers will] say "Oh this person received this [grade]"* - I6

Unauthorized Access: Parents mentioned the potential of systems being hacked. Some of these parents felt resigned that this as an inevitability. As (I9) put it: "Everybody gets hacked." Another parent, (I13) concurred: "In a phishing world, it may be impossible to keep that information private."

In addition to phishing, some parents also recognized the risks of e.g. public WiFi:

> *[Schools] shouldn't be [going through student information] on like public WiFi because... [then] it could fall in the hands of anybody.* -I5

Another parent highlighted a physical security flaw, noting that because visitors aren't escorted to their destinations, they could potentially gain access to on-site servers:

> *The school servers are in the school...and sometimes IDs don't get properly checked...it's not like the security officers are calling the office [saying] so and so person is coming up now.* -I4

4.3 Security Incidents

4.3.1 Zoombombings

Only three parents had actually experienced a zoombombing, an incident in which an uninvited individual or group disrupts

an online meeting[2], but most participants had at least heard of them either from other parents who have experienced it, the news, or guidance from the DOE. Those that have experienced zoombombings all described their child as actually having been exposed to inappropriate content, mostly in the form of posting "*disrespectful content in the chat (I2)* and "*trolling (I14)*". In some cases, however, the content was more explicit:

> *We did have that, the zoom bombing...all of a sudden, there was a naked guy in math class* - I10

For some parents, these incidents caused them to keep their child's camera off long-term:

> *We had recorded [the incident] and we shared it with the teacher...Ever since, I told my kids to have their cameras off.* - I4

4.3.2 Data Breaches

Two parents specifically mentioned the Illuminate Data Breach [15]. One found out from an article released by the DOE, while the other saw a note that their child had brought home while disposing of papers. While neither knew the details of the breach, they did know that their children's data had been leaked. Interestingly, both parents associated the breach with the DOE and *not* Illuminate. As a result, (I2) reported asking the DOE how they would remedy the situation and what information specifically was leaked. While (I2) described dissatisfaction with the DOE's reply that they didn't "*have answers for you right now*," a second parent however expressed resignation instead:

> *I honestly don't even pay attention because, you know, all that data is probably out there somewhere anyway: your child's birthday, your child's grades...it's all right there.* -I9

4.3.3 Inappropriate Content Sharing

While some security incidents and concerns involved parties outside the school, incidents involving the school community were also of note. For example, one parent recalled an incident severe enough that law-enforcement got involved:

> *There were some inappropriate things being air-dropped from some students to other students and, like the FBI had to be involved.* - I5

As a result, the air-drop capability was removed from DOE iPads altogether. One parent described another instance in which a security incident led to a loss of functionality:

> *Someone got access to a teacher's page...[and posted] really inappropriate work and they had to shut the whole system down.* - I1

Other parents also described incidents such as parents discussing sensitive information while their child's microphone was unmuted, children appearing under-dressed on camera, and parents visibly drinking alcohol.

4.4 Security Knowledge and Preferences

While parents differed in their security knowledge and preferences, they also described substantial uncertainty around technology and how data is handled. Especially parents who did not feel well-versed with technology, were unsure of what technology of its capacities - and therefore the threats it could present. According to one parent who used their personal laptop to manage their child's school account:

> *It's not that we have anything to hide, but we have our bank account information or bank statements, my credit card statement...my fear is that I'm not well [enough] versed in technology.* - I4

Even parents who did feel well-versed in technology expressed similar worries, however, as described in 4.2.5.

Another source of uncertainty for parents was digital tools' terms of service:

> *Everybody just kinds of scrolls to the bottom, presses yes, but what you don't realize is that in those terms and conditions like this is open to anybody...you're entering at your own risk.* - I17

While some parents mentioned this as common practice, one parent noted that the urgency they felt to adopt a new platform prevented them from scrutinizing these documents further:

> *We were in such a rush to get in, you probably didn't spend much time reading [the ToS] and so we may have agreed to things that we should have thought about a little bit more.* -I14

Parents were also unsure what mechanisms were in place to protect their children's data. While many participants mentioned "firewalls," not all of them were confident they were in place.

Not being confident who had access to their children's data contributed to concerns that it may be used inappropriately, as discussed in 4.2.5. Some concerns went further, however, with one parent worried that technology trouble could lead to attendance problems that could be used against families, citing incidents where a child's attendance record led to Child Protective Services (CPS) being called:

> *[Schools have used attendance data] in CPS cases...On one side right there is community concern right?..But on the other, for family to feel*

[2]Though, it was colloquially termed "zoombombing", not all parents experienced this phenomena on Zoom, one had had this occur on Google Meets

threatened with CPS action is also [a problem]. - I4

4.4.1 Lack of Guidance

Parents felt that technology adoption in the schools was rushed and there was a lack of training not only for them, but also for children and teachers:

> *They'll throw you an iPad or a Chromebook but...does a parent actually know how to use it? Does the kid actually know how to use it? Does the teacher know how to actually use it?* - I1

While some families were already familiar with certain applications, for others it was their child's —and sometimes parents'—first experience with these tools, with children teaching their parents how to use the applications in some instances.

Parents were also worried that schools and educators may not know the best security practices, thus putting their children at risk. Thus, while parents understood the challenges of the sudden transition to remote learning, they felt that the DOE should've invested more in educating their educators when it became clear that remote learning would continue:

> *There was a whole summer for [the DOE] to help their educators learn more technology...I just think that there was, you know, very little effort from the DOE* - I3

Another parent specifically wanted guidance on how to clean up the digital footprint left by remote learning:

> *Everybody's relying on Google to be good and delete the accounts...[but] I never got a notification from the school to go and delete your accounts or do any of this and everything that we set up on Google is still there floating around somewhere online.* - I3

Two parents brought up concerns that those whose primary language was not English would have trouble using the technology.

> *Students that are learning English or families whose primary language is not English were definitely not considered at all during this whole pandemic. There were families that [had] zero clue on how to go ahead and login to email* - I4

> *It's still difficult for me, I mean what about other parents?...You have a family that doesn't speak English, they would have no clue what they're doing* - I1

Parents also worried that their lack of knowledge would create future disparities between them and parents who had the resources to advocate for themselves.

4.4.2 Reactive vs Proactive

Parents felt that policies around technology were "reactive instead of proactive," with, the DOE only acting to fix problems after they arose. This left parents with the impression that things were not "thought through" on the educator's side. At least one parent (I14), however, felt that technology was inherently reactive, and sympathized with the challenge of anticipating unknown unknowns: "Technology is so reactive, you know you think you've got it until you don't."

4.5 Percieved Security Risk Mitigations

Reasons parents gave that mitigated concern with regards to privacy came down to (1) parents felt the information the applications had was not sensitive, (2) parents perceiving that their information was safe, (3) parents wanted the DOE to monitor their children's activities, (4) parents felt that exposure of data was normal and harmless and (5) parents trusted their school or their institution.

4.5.1 Uninteresting Data

Some participants felt that the information collected was harmless, and mentioned that they believed aggregated data was fine as you could not associate it with any individual students. Parents also felt that companies had or collected only a limited amount of information on students and that their privacy was protected because the applications don't collect what they viewed as highly sensitive information:

> *There's not like any sharing of any OSIS numbers from the DOE or any addresses or any social security number or anything like that. No nothing, besides, our name and email.* - I15

Another parent shared a similar sentiment:

> *There's no personal information on there. I mean, obviously I guess her OSIS number...but I mean other than that, I feel extremely secure* -I5

Still another put it even more bluntly:

> *If there was a breach, what are they going to do? Take her homework?* - I6

4.5.2 Perceived Safety

Just as some parents felt concern due to lack of technical knowledge, others felt safe for the same reason. These parents operated under the assumption that their children's information was secured as a default. As I14 states:

> *We didn't know not to feel safe...we just assumed that it was fine until it wasn't.*

Another parent assumed that digital information would be protected similar to analog information by default:

> *I assumed that [digital data is] just not shared at all...Like it's a virtual classroom but it stays in the classroom.* - I10

Still another said:

> *I was never concerned, but then again I don't I don't know too much about Google classroom and...I don't know, maybe I would be more concerned [if I knew more.]* -I7

Some parents were also reassured by certain security measures they observed, such as password protected zoom calls, restrictions on iPads, etc.:

> *I would have been a lot more uncomfortable using it if I didn't know about some of the settings that Apple has that allow you to restrict it even more* -I7

One parent mentioned feeling secure because of prior experiences with Google products, e.g. Google notifying them if someone was trying to get into their Google account. As a result, they believed they would know if there were notable security incidents involving school systems and technologies.

One parent even cited the "circuitous" login process for some applications (because they're were tied to DOE emails) contributing to their sense that the system would be impenetrable to outsiders.

Parents mentioned having taken their own precautions that kept their mind at ease. Some parents compartmentalized their children's activities, keeping personal activity off DOE devices so that they felt that their children's DOE device was free from personal information. Parents also coached their children to not overshare or disclose sensitive information.

> *I make sure that my kids are not using any other email address that is not connected with the school...everything in their iPad is school-related* - I2

4.5.3 Desire for Monitoring

Parents felt unconcerned about potential monitoring, in fact some parents felt that it was the DOE's duty to know what students were doing on DOE issued devices. One parent (I9) specifically mentioned that while yes, a child's data could be used against a child, they were unbothered because at their job, monitoring application and device usage was the norm, and thus the DOE monitoring children was "*what they're suppose to be doing*". Some parents felt that monitoring their children's activities would be beneficial to their learning as educators would know what weaknesses students had:

> *I think that [schools] should [monitor more], to be honest, because that way, it could tell them what [students] need to work on...If its school app based like the Zern, like the Raz-Kids or the Epic, I think it should be monitored.* - I17

Others were concerned their children would access inappropriate content and wanted to be made aware if it had occurred. As one parent put it:

> *If my son, even by accident [did something] that was inappropriate...I would want someone to email me, or give me a phone call or something* -I7

4.5.4 Normalization of Data Breaches and Disclosure

As mentioned in 4.3 some parents believed data exposure was inevitable, with others adding that they felt that such breaches were not a cause for concern because they could protect themselves (e.g. by changing their passwords):

> *What's the big deal if there's a breach or something? You're informed, and you can change your password.* - I7

Parents felt that because they often sign disclosure forms, that were used to their children's data being collected.

4.5.5 Institutional Trust

Parents mentioned their trust in the school and educators' intentions and capability as a reason they were or weren't concerned about their child's safety. Some parents felt that the applications were safe to use because the DOE had authorized the use of these applications.

> *These [applications] are educational...they're picked by the DOE, and [so] you know that they can be trusted.* - I10

Others specifically trusted in the capabilities of their school's IT personnel to protect their children:

> *[We] hear what he's doing and all the safety tools that he has been using to make sure that everyone's information is protected and it's not going to be leaked in any way somehow. So I think having the conversation with him makes me feel a little bit better.* - I2

How Trust is Built and Lost: Participants cited transparency, constant updates/contact, perceived competence, intent, following through on promises and generally feeling as if administrators were working together with families as factors that contributed to trust in their institution. Communication was the factor that almost all participants expressed influenced their trust in the school. Aside from lack of communication,

almost unanimously, participants expressed that their trust would decrease were a data breach to occur.

Participants often trusted their school more than the DOE, whom most trusted tentatively.

> *I see DOE as a political institution...[whereas] I know the school, I know the principal...I'd be more surprised if it turned out that the school didn't protect the kids. If the DOE didn't protect kids privacy I'd be less surprised.* - I10

Parents trusted the DOE less not only due to lacking the contributing factors to trust but also cited decisions made by the current leaders regarding policies surrounding funding and COVID and lack of families' input on decisions.

> *I wouldn't be surprised if there was something huge that came out about all New York City school kids* - I3

> *I don't have confidence in what [the Chancellor] says just from the sheer lack of COVID concerns. You telling me that you've got families input, but not telling me what families, from what district...Your changing school lunches from one day to another without input is not getting my trust.* - I4

> *Eric Adams talking about how he's going to do testing for dyslexia. I'm like: you're gonna do testing for dyslexia, but you're also playing down the budget? I would like to see how that works.* - I8

Parents saw the DOE as the governing body whereas the schools were just facilitators of the technology. Thus they felt the blame should be on the DOE rather than the school.

> *The DOE...[is] essentially responsible for all of this stuff...They're the ones rolling out the technology. The school staff, they're really just facilitators.* - I14

When asked what they would do if they lost trust in the school, a common sentiment among participants was that: depending on the severity of the breach of trust, they would either bring up the issue to the school or in the worst case transfer schools. Parents acknowledged that they felt that their schools were doing the best that they could given the circumstances. Some felt this way because they had not heard about any data breaches or incidents that had occurred in their school. In the words of I14:

> *I think [the schools] did what they could and it seemed to be sufficient because there weren't any breaches. So you had to assume that they had done a lot on the back end.*

There were also parents who expressed resignation in that due to the need for their children to continue learning, and in doing so, they chose to trust the software and technology used. In the words of I10:

> *There's no alternative to it. So I went with it, and I decided to believe that it's safe, but I don't know how protected the kids were actually*

Or as I14 put it: "*We just sort of crossed our fingers and assumed that everything was going to be okay.*" and *I haven't been burned yet [...] There's so much going on, that I just I sort of packed that away and so I'm going to trust this until it burns me.*

5 Discussion

Parents' concerns with technology used in the classroom were consistent with prior work regarding children's technology use in general [58, 79, 80]. One difference however, was that in the context of general internet usage, parents' concerns regarding loss of information control often revolved around children's self-disclosure of information [77, 79], whereas in the educational context, parents expressed loss of information control in terms of others inappropriately accessing their children's information either through indiscretion or "hacking".

Much like Sun et al.'s findings, parents' concerns were often informed by (1) having experienced or heard of incidents, and (2) the amount of familiarity they felt with technology in general [70]. However, while Sun et al. find that those who self-describe as tech-savvy are more attuned to potential privacy risks [70], our findings indicate that those who feel they were not well-versed with technology were just as aware of potential privacy risks. For parents who felt they were familiar with the technology, their concerns were informed by what they believed technology to be capable of. Whereas parents who felt they were less familiar's concerns were informed by their uncertainty around what technology was capable of.

Parents' concerns were mitigated by (1) their beliefs that the information schools and applications had were uninteresting and would not identify their child personally, (2) their beliefs that these applications were generally safe to use—informed by their trust placed in their schools to keep their children safe. Parents also expressed a desire for the school to monitor their children, thus feeling more comfortable with schools surveilling their children's school devices and accounts. In addition, parents were also more tolerant of security risks due to the prevalence of incidents and being desensitized to data collection and disclosure.

It is interesting to note that while we primarily asked about privacy, parents often framed privacy in terms of security incidents and concerns. This makes sense as we allowed parents to answer based on their own conception of privacy which aligned with some privacy concerns, but also some security concerns. These security concerns seem to indicate that parents view privacy through a lens of shielding their children and their data from outside threats rather than regulating the information shared.

5.1 The Need For Accessible Documentation and Meaningful Choices

The lack of familiarity with the technology used creates an excess burden of having to make decisions and acquiesce to their children using systems they do not understand. Our findings indicate that parents were not given informed choices in the adoption of technology in the classroom, but the onus was still on the parents to manage their children's accounts. This problem has been documented since 2017 and still has not been meaningfully addressed by schools and administration [27]. Additionally, parents pointed out that the information that they are given is inaccessible to families for whom English is not their primary language.

5.1.1 Lack of Accessible Documentation

While privacy documentation exists, because they are not presented initially, the burden lies on the parents to seek them out. Additionally, even when parents find the documentation, such documents i.e. privacy policies and terms of service, are often lengthy and arcane [50]. This combined with the swiftness schools adopted technology makes it difficult for users to be informed of the risks before using applications, let alone raise concerns to the schools—especially for whom English is not their primary language.

> *It's scary for a family right and if you don't know the language, it's worse.* - I4

We took a look at the privacy policies of some of the applications parents stated their children have used; while some applications like Zoom do have their policies in multiple languages [6], other applications like iReady and Google for Education do not [4, 5] even though English is the predominate language in only 65% of NYC households [9]. However, the applications that do have multilingual policies do not outright present different language options. Zoom's website requires users to scroll to the bottom to the "language" option written in English and select their preferred language. This is a serious usability issue because those not familiar with technology may not even know this option exists as it is hidden all the way at the bottom. Studies have shown that users often do not pay attention to information on the lower portions of a website [18, 24, 30]. More pressingly, those who don't understand English *will not* know what that dropdown menu is for let alone change it. While programs such as Common Sense's privacy program distill privacy policies to be more understandable for the average person, resources are only available in English and Spanish, with the similar fault that the language selection choice is by default presented in English [20].

5.1.2 Lack of Meaningful Choices

Parents are not afforded choices when it comes to what is used in the classroom. While some parents claim that they could opt-out should they raise a serious concern, because they are not presented information upfront and available information is often inaccessible to those who are not technically savvy or are non-English speakers, it can be difficult for parents to understand the risks let alone know to advocate for themselves and their children. Even if parents were able to opt-out, there may be a lack of alternatives in schools where technology has been integrated. Gebhart et al found that even when schools allowed for opt-ing out of the use of technology, many schools lacked any alternative [27]. Indeed, while an alternative existed on paper for some of the interviewed parents, this alternative was wholly inconvenient or reserved for extreme cases. Moreover, accounts are created for students by default—thus even if parents have opted out, some information has already been disclosed. Thus the agency that parents are afforded is essentially meaningless.

5.2 Delegation of Trust and Responsibility

Our research supports Gebhart et al.'s conclusions that parents lack agency regarding their children using technology in schools [27]. However, our qualitative methods revealed that the delegation of trust to schools mitigated concerns parents had with such technologies. Indeed, our results suggested that parents trusted the applications used in schools because by sending their children to schools they had already placed their trust in the schools to keep their children safe. Because of this delegation, they trusted that technology choices are made for the benefit of their children and have been thoroughly vetted by the DOE to be safe. However, it is important to note that due to technology being mandatory, though parents did choose to trust their schools, their trust was also necessitated by the fact their children needed an education. This idea of delegation of responsibility to another institution is not a new one. This dynamic is similar to the trust between medical professionals and patients whereby individuals trusted those with more expertise to make decisions for them.

However, a question must be raised whether this trust is warranted. Applications do require an audit from the DOE approved for usage in the classroom [59], there is lack of transparency in what qualifies to be a DOE approved application aside from compliance with regulations which as outlined in 2.4 can be rife with loopholes. Passing an audit, however, still does not ensure that the application is secure. The original application used to conduct synchronous classes—Zoom—was later banned from usage following security incidents. RazKids, a reading application that many parents reported having used, did not encrypt teacher and parents' accounts, a security flaw that could expose students' PII [65]. Regarding the Illuminate data breach, officials claim that Illuminate misrep-

resented the security measures it had in place—specifically that Illuminate also did not encrypt students' data as they had claimed [21, 36], suggesting that audits do not verify vendor's claims regarding security practices. This arguably indicates that aside from making sure application vendors are following regulations, the DOE themselves are delegating the responsibility to the vendors to be responsible with and protect the data they provide to these companies.

Parents believed that minimal information was shared with third-party companies, however in light of the Illuminate data breach, it is clear that schools actually share a lot of information with vendors including IEP statuses—a piece of information parents believed to be highly sensitive [55]. While parents focused mostly on data shared with third-party companies, with exception of parents with children with IEPs parents did not mention information provided directly to the school as being at risk. However, schools require parents to disclose a lot of PII to even register their children for school which can also be exposed if schools themselves were attacked such as in the case of the ransomware attack in Los Angeles [35]. This could be because data used for IEP is intrinsically tied to medical data, is individual to each student, and the data collection is more continuous while registering for school or an application is a one-time process and parents believed that the information would only be used in aggregate.

It is interesting to note that while the Illuminate data breach affected 820,000 students in NYC, only two parents mentioned it, both of whom seemed to have stumbled on the information incidentally. While one of the parents did receive notice from the school directly, it clearly did not communicate importance as they had only reviewed the content while *throwing out old papers* (I9). Moreover, news reported that many parents in New York State (NYS) assumed that the notification of the data breach from Illuminate itself was an attempted scam [23]. It is clear that the disclosure of the Illuminate data breach was inadequate at reaching those who may have been affected. Parents indicated that because schools communicated whenever any problems arose, parents trusted that in absence of this, there was no cause for concern. Thus this lack of effective communication, therefore, lulls parents into a false sense of security.

5.3 Normalizing Loss of Privacy

Our findings indicate that during the transition to online learning, there was an assumption by the DOE that everyone knew how to use the devices and applications when this was certainly not the case. For most children and even some parents, remote learning was their first experience with using these technologies. In fact, a report released by the state comptroller indicated that 16% of households in New York City did not have access to the internet in 2019—these households tended to be families of lower income [10]. Additionally, NYC also has a large population of students whose parents do not speak English [34]. The lack of internet access and language barriers prevalent in the NYC community indicate that lack of familiarity with technology especially those used in schools for remote learning is a widespread problem that affects not only learning but also privacy and security awareness.

The behaviors that children learn are the ones they will follow them as they grow. Individuals' first experiences often influence future decision making, a phenomenon known as anchoring [2]. As children do not control their own privacy, these experiences may leave children under-equipped to control their own privacy or worse, teach children bad practices. If bad practices are reinforced at a young age, this will affect them later in life when they use technology not only for educational usage but personal usage. Lack of control over one's privacy might also lead children to feel disempowered and as a result disengage from attempting to have control over their own privacy [45]. This will negatively impact the digital literacy in the population going forward as there will be more people who engage in practices that may introduce insecurities in both privacy and security. As indicated from our findings children's usage of technology is also how some parents get educated in the applications used and as such bad security habits may actually be passed on not only from parent to child but from child to parent.

5.3.1 Normalization of Incidents

As suggested by our findings, parents have already come to expect security incidents to occur and thus have a higher risk tolerance of things like phishing, and data breaches as stated by I9 in 4.3.2. However, parents who are concerned when security incidents happen find that they are not given guidance on how they could remedy their situation. This can be harmful as it could lead to learned helplessness wherein because both parents and their children feel resigned to the inevitability of their information being exposed or accessed without recourse, they may not even attempt to prevent these incidents. This can create a feedback loop wherein users prioritize protecting their privacy less leading to more incidents.

5.3.2 Normalization of Surveillance

There also exists a tension between the expectations of the school to monitor children and children's right to privacy. Some parents expected that schools monitored all activities of students. Circling back to this being a formative experience for children, children being used to excessive monitoring and data harvesting will grow up with this expectation—much like the one parent who felt surveillance was the norm due to being surveilled at work. Safety is often cited as a justification for surveillance, however, schools surveil students not only for possible safety concerns, but also minor infractions such as truancy—which one parent mentions led to a family having CPS called on them. In addition, there is also no evidence

that surveillance is effective as a safety measure [28]. Indeed, studies have found that the best way to protect children from online harms is to teach children how to protect themselves from these harms [22, 77, 78]. What's more, because the large amount of data collected is stored indefinitely, and the threat of data breaches is prevalent, it can be argued that surveillance can pose a safety risk in itself. This is especially true when surveillance extends outside of schools. Shade and Singh found that the privacy policies of this type of software is often unclear on whether they only collect information on the student, or whether they cross-reference the student's information with that of their social network [64]. Thus, this risks the privacy not only of students, but also those in their social network. Moreover, the effects of surveillance may counteract the intended purpose of school—to provide an environment that fosters learning. Students may fear asking questions or looking up information due to fears of embarrassment, or worse punitive action, the latter of which disproportionately affects students who are minorities [41, 47, 63, 64, 74].

5.4 Recommendations

5.4.1 School Administrators and Educators

Obtain Informed Consent from Parents: It is clear that there exists a need for parents to have the ability to make meaningful informed choices. As we are no longer in emergency remote learning, there is less of an urgency to quickly adopt technology. In addition, parents often mentioned being asked to consent to their school using photos of their children by filling out photo release forms, therefore it is clear that schools do have avenues to obtain expressed consent. Therefore, parents should be informed ahead of time and presented with adequate and accessible notice and disclosure before introducing any technology.

> *I think if we knew in advance: "Here are the things your students going to be using this year, please familiarize yourself with it" a lot of their parents would have probably found no issue. Which is [why] being given that opportunity would have been nice.* - I14

Moreover, this notice should be recurring as (1) privacy procedures change, and (2) because different teachers may use different tools, it cannot be assumed that parents have already had notice. Accounts should not be created until parents consent. Schools should also be prepared to offer alternatives for those who do not or have revoked their consent. These alternatives should not require substantially more work for parents, children, and educators to access.

Better Communication with Parents: Parents should not have to be cybersecurity experts to ensure their children are protected. Delegation of trust is not a bad thing, but schools should earn that trust by not only better communicating to parents, but also making sure that they *are* protecting students in practice. Our interviews demonstrated that the trust parents have in schools transfers to their treatment of data, privacy, and security. It is possible that poor handling of these issues could lead to more general mistrust in schools and school systems.

5.4.2 Educational Leaders

Working With the Security Community: Given that educational bodies are underfunded and lack the resources to invest in cybersecurity [33, 51], it is important that the security community help schools be worthy of the trust parents give them. One avenue could be to conduct independent audits of applications used in schools similar to Common Sense Media's privacy program [20]. However, this should extend past only distilling security and privacy claims made by companies, but also verifying claims as companies may misrepresent them. Moreover, these independent audits could also identify and provide guidance on what information is strictly necessary for applications to perform its tasks, and what information is not. Educational leaders in turn should take findings and guidance from independent audits seriously. Moreover, though the law allows schools to share information with vendors of educational technology as if they were school officials, we urge educational leaders to treat these companies as if they were not.

Adding Digital Literacy to Existing Curricula: While throughout this paper we center parents and their concerns, these concerns are mostly about their children's data and safety. As these children will become digital citizens, it is also important to teach and empower them to make good decisions for themselves as well as build resiliency against online risks especially as children are already leaving digital traces through their use of classroom technology [22, 77]. As such, we emphasize the importance of fostering digital literacy in the educational space starting at an early age. We suggest that digital literacy courses be incorporated into existing curricula. While there are already some initiatives in schools to teach children about digital safety i.e. cyberbullying and self-disclosure of information, given the prevalence and potential harms that can come from datafication, digital literacy education should also include an understanding of data collection—not only what is collected, but how data is used and can move around the internet as well as potential harms that can result [68, 69, 76].

5.4.3 Academics

Given that expressed consent seemingly is easy to obtain, future research should seek to understand why administrative bodies choose not to do so and how transparency could be encouraged.

Regarding the Illuminate data breach, it is clear that the

incident was poorly communicated to parents. It is beyond the scope of the paper to determine how best to disclose data breaches and other incidents, this is an area that needs to be further studied by the security community. However, schools routinely contact parents for consent for other activities (field trips, photos) and have the capacity to contact parents when other incidents occur (for example, a sick child). These mechanisms might be used to better communicate security and privacy incidents to parents.

6 Conclusion

After COVID-19's move to remote learning, schools and educational technology vendors became a target for cyberattacks.We wanted to know what concerns parents had with regards to their children using technology in the classroom and whether they were aware of the associated risks. Our results indicated that while parents had some concerns, these concerns were mitigated by their trust in schools to keep their children safe—which extended to parents desire for their schools to monitor their children. While parents cited communication and family input as a big factor in trust in their schools, we found that parents were not informed, not given guidance nor meaningful choice about the technology that would be used in their children's education. Parents were also under-informed on security incidents that had occurred. Moreover, while parents believed that schools shared minimal and non-sensitive information to applications used, evidence from incidents such as data breaches indicate otherwise. This all indicates that educational bodies need to do better to earn the trust that parents place in them by better communicating incidents and allowing parents informed choice regarding technology use. In addition, educational leaders, in tandem with the security community should make sure that applications used *are* actually safe.

7 Acknowledgements

We would like to thank the parents who participated in this study as well as the anonymous reviewers who provided constructive feedback. The first author was supported by a US Department of Education GAANN Fellowship (#P200A210096).

References

[1] https://calendly.com/.

[2] Anchoring bias. https://thedecisionlab.com/biases/anchoring-bias.

[3] Doe data at a glance. https://www.schools.nyc.gov/about-us/reports/doe-data-at-a-glance.

[4] Explore faqs about google for education's commitments to keep your data secure and provide a safe digital learning environment for school communities. https://edu.google.com/intl/ALL_us/why-google/privacy-security/frequently-asked-questions/.

[5] i-ready® platform data handling and privacy statement. https://www.curriculumassociates.com/support/privacy-and-policies/i-ready-data-handling-privacy.

[6] Zoom privacy statement — zoom. https://explore.zoom.us/en/privacy/.

[7] Family educational rights and privacy act of 1974 20 u.s.c. § 1232g; 34 cfr part 99, 1974.

[8] Children's online privacy protection rule 15 u.s.c 6501-6508. https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312, 1998.

[9] How many languages are spoken in the new york area. https://www.worldatlas.com/articles/how-many-languages-are-spoken-in-nyc.html, Aug 2020.

[10] Dinapoli: Over one million new yorker households are not connected to broadband. https://www.osc.state.ny.us/press/releases/2021/09/dinapoli-over-one-million-new-yorker-households-are-not-connected-broadband, Sep 2021.

[11] Parent and parent teacher associations. https://www.schools.nyc.gov/get-involved/families/parent-associations, 2023.

[12] ADAM, S. The state of ransomware in education 2021. https://news.sophos.com/en-us/2021/07/13/the-state-of-ransomware-in-education-2021/, Jul 2021.

[13] ARUM, R., AND STEVENS, M. L. Under digital surveillance: how american schools spy on millions of kids. *The New York Times* (Mar. 2020).

[14] ATTENEDER, H., AND COLLINI-NOCKER, B. Under control: Audio/video conferencing systems feed "surveillance capitalism" with students' data. In *2020 13th CMI Conference on Cybersecurity and Privacy (CMI) - Digital Transformation - Potentials and Challenges(51275)* (Nov 2020), p. 1–7.

[15] BAMBERGER, C. Nyc schools ban use of illuminate education products after massive data breach. *New York Post* (May 2022).

[16] BANKS, C. Re-identification of "anonymous" data is scarily simple. https://anonyome.com/2020/12/re-identification-of-anonymous-data-is-scarily-simple/, Dec 2020.

[17] BONINGER, F., AND MOLNAR, A. Learning to be watched: Surveillance culture at school.

[18] BURRELL, A., AND SODAN, A. Web interface navigation design: Which style of navigation-link menus do users prefer? In *22nd International Conference on Data Engineering Workshops (ICDEW'06)* (2006), pp. 42–42.

[19] COHNEY, S., TEIXEIRA, R., KOHLBRENNER, A., NARAYANAN, A., KSHIRSAGAR, M., SHVARTZSHNAIDER, Y., AND SANFILIPPO, M. Virtual classrooms and real harms. *CoRR abs/2012.05867* (2020).

[20] COMMON SENSE MEDIA. Privacy program. https://privacy.commonsense.org/.

[21] CONSOLE JR, R. Data breach alert: Illuminate education. https://www.jdsupra.com/legalnews/data-breach-alert-illuminate-education-2802445/.

[22] DUERAGER, A., AND LIVINGSTONE, S. How can parents support children's internet safety?

[23] EDWARDS, J. No, that data breach letter from illuminate education is not a scam. https://patch.com/new-york/newrochelle/no-data-breach-letter-illuminate-education-not-scam, Jun 2022.

[24] ESPIGARES-JURADO, F., MUÑOZ-LEIVA, F., CORREIA, M. B., SOUSA, C. M. R., RAMOS, C. M. Q., AND FAÍSCA, L. Visual attention to the main image of a hotel website based on its position, type of navigation and belonging to millennial generation: An eye tracking study. *Journal of Retailing and Consumer Services 52* (Jan 2020), 101906.

[25] FEATHERS, T. Proctorio Is Using Racist Algorithms to Detect Faces.

[26] FRANCESCHI-BICCHIERAI, L. How Ransomware Is Causing Chaos in American Schools.

[27] GEBHART, G. Spying on students: School-issued devices and student privacy. https://www.eff.org/wp/school-issued-devices-and-student-privacy, Apr 2017.

[28] GEBHART, M. W., AND GENNIE. Schools are pushing the boundaries of surveillance technologies. https://www.eff.org/deeplinks/2020/02/schools-are-pushing-boundaries-surveillance-technologies, Feb 2020.

[29] GLASER, B. G., AND STRAUSS, A. L. The purpose and credibility of qualitative research. *Nursing research 15*, 1 (1966), 56–61.

[30] GOLDBERG, J. H., AND LEWENSTEIN, M. Eye tracking in web search tasks: Design implications.

[31] JENSEN, C., AND POTTS, C. Privacy policies as decision-making tools: An evaluation of online privacy notices. 8.

[32] JENSEN, C., POTTS, C., AND JENSEN, C. Privacy practices of internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies 63*, 1–2 (Jul 2005), 203–227.

[33] JONES, D. K-12 schools lack resources, funding to combat ransomware threat. https://www.cybersecuritydive.com/news/k12-ransomware-target/636474/.

[34] JORGENSEN, J. Advocates: Schools need more funding to communicate with immigrant families. https://www.ny1.com/nyc/all-boroughs/news/2022/06/09/advocates–schools-need-more-funding-to-better-communicate-with-immigrant-families.

[35] KAPKO, M. Los angeles schools' data leaked after ransomware attack. https://www.cybersecuritydive.com/news/los-angeles-schools-ransomware-leak/633177/.

[36] KEIERLEBER, M. After huge illuminate data breach, ed tech's 'student privacy pledge' under fire. https://www.the74million.org/article/after-huge-illuminate-data-breach-ed-techs-student-privacy-pledge-under-fire/, Jul 2022.

[37] KELLY, G., GRAHAM, J., BRONFMAN, J., AND GARTON, S. Privacy risks and harms the common sense privacy program. Tech. rep., Common Sense Media, 2019.

[38] KIRLAPPOS, I., PARKIN, S., AND SASSE, M. A. Learning from "shadow security": Why understanding non-compliance provides the basis for effective security.

[39] KOPPEL, R., SMITH, S., BLYTHE, J., AND KOTHARI, V. Workarounds to computer access in healthcare organizations: you want my password or a dead patient? In *Driving Quality in Informatics: Fulfilling the Promise*. IOS Press, 2015, pp. 215–220.

[40] KRUTKA, D., SMITS, R., AND WILLHELM, T. Don't be evil: Should we use google in schools? *TechTrends 65* (03 2021).

[41] KSHETRI, N. School surveillance of students via laptops may do more harm than good. http://theconversation.com/school-surveillance-of-students-via-laptops-may-do-more-harm-than-good-170983, Nov 2021.

[42] KUYKENDALL, K. 565 schools, over 1m students in ny impacted by illuminate data breach, nysed says; 2nd colorado district notifies parents. https://thejournal.com/articles/2022/05/05/565-schools-over-1m-students-impacted-by-illuminate-data-breach-2nd-colorado-district-affected.aspx.

[43] LAIRD, E., GRANT-CHAPMAN, H., VENZKE, C., AND DE LA VALLEE, H. Q. Report – Hidden Harms: The Misleading Promise of Monitoring Students Online.

[44] LAURICELLA, A. R., AND CINGEL, D. P. Parental influence on youth media use. *Journal of Child and Family Studies 29* (2020), 1927–1937.

[45] LIVINGSTONE, S., STOILOVA, M., AND NANDAGIRI, R. Growing up in a digital age.

[46] LU, A. J., DILLAHUNT, T. R., MARCU, G., AND ACKERMAN, M. S. 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), 1–26.

[47] LU, A. J., MARCU, G., ACKERMAN, M. S., AND DILLAHUNT, T. R. Coding bias in the use of behavior management technologies: Uncovering socio-technical consequences of data-driven surveillance in classrooms. In *Designing Interactive Systems Conference 2021* (New York, NY, USA, 2021), DIS '21, Association for Computing Machinery, p. 508–522.

[48] MANOLEV, J., SULLIVAN, A., AND SLEE, R. The datafication of discipline: Classdojo, surveillance and a performative classroom culture. *Learning, Media and Technology 44*, 1 (Jan 2019), 36–51.

[49] MARK, J. No more snow days? nyc schools say remote learning eliminates the need. *Washington Post* (Sep 2022).

[50] MCDONALD, A. M., AND CRANOR, L. F. The cost of reading privacy policies.

[51] MCKENSIE, L. State edtech leaders say schools have insufficient cybersecurity funding. https://statescoop.com/state-edtech-leaders-schools-insufficient-cybersecurity-funding/, Sep 2022.

[52] MORRISON, S. Google's education tech has a privacy problem. https://www.vox.com/recode/2020/2/21/21146998/google-new-mexico-children-privacy-school-chromebook-lawsuit, Feb 2020.

[53] MORSE, J. M., FIELD, P. A., MORSE, J. M., AND FIELD, P. A. The purpose of qualitative research. *Nursing research: The application of qualitative approaches* (1996), 1–17.

[54] NARAYANAN, A., AND SHMATIKOV, V. How to break anonymity of the netflix prize dataset. arXiv:cs/0610105.

[55] NEW YORK CITY DEPARTMENT OF EDUCATION. Data security incidents. https://www.schools.nyc.gov/about-us/policies/data-privacy-and-security-policies/data-security-incidents.

[56] NEW YORK CITY DEPARTMENT OF EDUCATION. The iep. https://www.schools.nyc.gov/learning/special-education/the-iep-process/the-iep.

[57] NEW YORK CITY DEPARTMENT OF EDUCATION. 2019 - 2020 school locations.

[58] OATES, M., AHMADULLAH, Y., MARSH, A., SWOOPES, C., ZHANG, S., BALEBAKO, R., AND CRANOR, L. F. Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration. *Proceedings on Privacy Enhancing Technologies 2018*, 4 (Oct 2018), 5–32.

[59] OF EDUCATION, N. Y. C. D. Data privacy and security compliance process. https://infohub.nyced.org/in-our-schools/policies/data-privacy-and-security-compliance-process.

[60] PORTER, C. C. De-identified data and third party data mining: The risk of re-identification of personal information.

[61] POWER, R. Child identity theft. Tech. rep., Tech. rep., Carnegie Mellon CyLab., 2011.

[62] PULLANO, N. Nyc schools to cut remote learning for fall 2021. https://www.courthousenews.com/nyc-schools-to-cut-remote-learning-for-fall-2021/.

[63] RAIBLE, J., AND IRIZARRY, J. G. Redirecting the teacher's gaze: Teacher education, youth surveillance and the school-to-prison pipeline. *Teaching and Teacher Education 26*, 5 (Jul 2010), 1196–1203.

[64] SHADE, L. R., AND SINGH, R. "honestly, we're not spying on kids": School surveillance of young people's social media. *Social Media + Society 2*, 4 (2016), 2056305116680005.

[65] SINGER, N. Digital learning companies falling short of student privacy pledge. https://archive.nytimes.com/bits.blogs.nytimes.com/2015/03/05/digital-learning-companies-falling-short-of-student-privacy-pledge/, 1425574440. Cad: 0.

[66] SINGER, N., AND CONGER, K. Google is fined $170 million for violating children's privacy on youtube. *The New York Times* (Sep 2019).

[67] SKOWRONSKI, D. S. Coppa and educational technologies: The need for additional online privacy protections for students. *Georgia State University Law Review 38* (2022).

[68] STOILOVA, M., LIVINGSTONE, S., AND NANDAGIRI, R. Digital by default: Children's capacity to understand and manage online data and privacy. *Media and Communication 8*, 4 (Nov 2020), 197–207.

[69] SUN, K., SUGATAN, C., AFNAN, T., SIMON, H., GELMAN, S. A., RADESKY, J., AND SCHAUB, F. "they see you're a girl if you pick a pink robot with a skirt": A qualitative study of how children conceptualize data processing and digital privacy risks. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, May 2021), CHI '21, Association for Computing Machinery, p. 1–34.

[70] SUN, K., ZOU, Y., RADESKY, J., BROOKS, C., AND SCHAUB, F. Child safety in the smart home: Parents' perceptions, needs, and mitigation strategies. *Proceedings of the ACM on Human-Computer Interaction 5*, CSCW2 (Oct 2021), 471:1–471:41.

[71] SWEENEY, L. Only you, your doctor, and many others may know. *Technology Science*.

[72] TERÄS, M., SUORANTA, J., TERÄS, H., AND CURCHER, M. Post-covid-19 education and education technology 'solutionism': a seller's market. *Postdigital Science and Education 2*, 3 (Oct 2020), 863–878.

[73] TROTTER, A. Market for K-12 Course-Management Systems Expands. *Education Week* (Feb. 2008).

[74] TUCKER, J. W., AND VANCE, A. School surveillance: The consequences for equity and privacy. https://www.nasbe.org/school-surveillance-the-consequences-for-equity-and-privacy/.

[75] WANG, A. Scrutinizing coppa: The privacy of our past, present, and future. *Joseph Wharton Scholars* (May 2022).

[76] WANG, G., ZHAO, J., VAN KLEEK, M., AND SHADBOLT, N. "don't make assumptions about me!": Understanding children's perception of datafication online. *Proceedings of the ACM on Human-Computer Interaction 6*, CSCW2 (Nov 2022), 419:1–419:24.

[77] WISNIEWSKI, P., JIA, H., XU, H., ROSSON, M. B., AND CARROLL, J. M. "preventative" vs. "reactive": How parental mediation influences teens' social media privacy behaviors. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work Social Computing* (New York, NY, USA, Feb 2015), CSCW '15, Association for Computing Machinery, p. 302–316.

[78] WISNIEWSKI, P. J., XU, H., ROSSON, M. B., AND CARROLL, J. M. Adolescent online safety: The "moral" of the story. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work amp; Social Computing* (New York, NY, USA, 2014), CSCW '14, Association for Computing Machinery, p. 1258–1271.

[79] ZHANG-KENNEDY, L., MEKHAIL, C., ABDELAZIZ, Y., AND CHIASSON, S. 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* (New York, NY, USA, Jun 2016), IDC '16, Association for Computing Machinery, p. 388–399.

[80] ZHAO, J., WANG, G., DALLY, C., SLOVAK, P., EDBROOKE-CHILDS, J., VAN KLEEK, M., AND SHADBOLT, N. '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* (May 2019), ACM, p. 1–13.

Notes

A Interview Guide

1. What age are your child(ren) and what grade(s) are they in?
2. How old are you?
3. Does your child go to public or private school?
4. What software/ devices are used for class during the pandemic? And now?
5. So let's talk about technology in general. How comfortable are you with using technology and software in general? What about specifically the technology and software for your child's education?
6. Was there an overlap in the accounts and devices used for school and personal and work activities? What were the circumstances?
7. Have (Could you recall a time) you had/(there been) any difficulties with regard to managing your child accounts both during remote learning and now?
8. Do you have access to your child's accounts both personal and educational?
9. Do you know if the school has access to/monitors your child's educational accounts/devices?
10. Would you be comfortable with the school monitoring your children's activities on their educational accounts? What about their personal accounts?
11. Do you know what the teachers could see?
12. Do you/your child get to choose what to use in school with regards to to applications and devices?
13. Were there any instances where you were uncomfortable with any of the applications used for class? Did the school do anything to remedy the situation or assuage your concerns?
14. Did schools offer a no tech option such as paper packets? If so, have you ever utilized no-tech option? Were there any specific reasons you chose to (not) use the no-tech option?
    If not, would you prefer they have a no-tech option? What are the reasons?
15. Are your child(ren)s' classes recorded? What do you feel are the benefits and drawbacks of this?
16. Would/Are you personally be comfortable with your child(ren)'s classes being recorded?

17. Were there any changes in policies or procedures with regard to technology from March 2020 until in-person lessons resumed? If so what were they in response to? Do you agree with these changes? What are your reasons?
18. What aspects of your child's education do you wish were different wrt the software/technologies used or policies surrounding them? What led you to feel this way? Was there any specific incident? (e.g. data breach)
19. Could you recall any moments where you or your child had to do something differently than instructed on an online platform for any reason?
20. Have(Could you recall a time when) you or your child ever felt that the software/ technology they use in school poses any privacy concerns? This could be to your child, you, or in general. What led you to feel this way? Was there any specific incident?
21. Can you recall any incidents where you wished that your child would have more privacy with regards to the use of their educational accounts/devices?
22. Were there any incidents where you wished that there was less?
23. To what extent do you believe your child's privacy is important with regards to school?
24. Are there certain categories of people and/or companies that you would feel uncomfortable having information about your child's classroom activities and performance?
25. Were there ever times during remote learning when you were surprised or upset to learn how or with whom information about your child's classroom activities or performance was being shared? (Did privacy or security concerns come up during remote learning?)
26. What are your expectations of privacy in the classroom? What information about your child's classroom activities and/or performance are OK to share outside the classroom or school? Would you prefer that the school ask your permission before sharing this type of information, or do you trust the teachers'/school's judgment about that?
27. How much trust do you have in your child's school to protect your child and their privacy?
28. How important do you think trust is to your organization?
29. What influences your trust in the school? Do you have any examples?
30. What privacy concerns do you have (if any) regarding the use of technology in general?
31. Is there anything I didn't ask that you'd like to share?