"They think it's totally fine to talk to somebody on the internet they don't know": Teachers' perceptions and mitigation strategies of tweens' online risks

Sana Maqsood
sana.maqsood@carleton.ca
Carleton University
Ottawa, Ontario, Canada

Sonia Chiasson
chiasson@scs.carleton.ca
Carleton University
Ottawa, Ontario, Canada

ABSTRACT

Teachers play a key role in educating children about digital security and privacy. They are often at the forefront, witnessing incidents, dealing with the consequences, and helping children handle the technology-related risks. However, little is reported about teachers' lived classroom experiences and their challenges in this regard. We conducted semi-structured interviews with 21 Canadian elementary school teachers to understand the risks teachers witness children aged 10–13 facing on digital media, teachers' mitigation strategies, and how prepared teachers are to help children. Our results show that teachers regularly help children deal with digital risks outside of teaching official curriculum, ranging from minor privacy violations to severe cases of cyberbullying. Most issues reported by teachers were the result of typical behaviours which became risky because they took place over digital media. We use the results to highlight implications for how elementary schools address digital security and privacy.

CCS CONCEPTS

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

KEYWORDS

digital literacy, security and privacy risks, children, teachers

ACM Reference Format:
Sana Maqsood and Sonia Chiasson. 2021. "They think it's totally fine to talk to somebody on the internet they don't know": Teachers' perceptions and mitigation strategies of tweens' online risks. In *CHI Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3411764.3445224

1 INTRODUCTION

Smart classrooms, equipped with smart-boards, educational technology platforms, such as Google Education, and Bring-Your-Own-Devices (BYOD), provide new learning opportunities to elementary school students. For example, students can use collaboration technologies to communicate and work with their peers on group projects, in-person or remotely. At the same time, the increased use of technology in schools and BYOD also introduce new security and privacy risks, and exacerbate existing risks [1, 32, 33, 47]. Students might use technology for non-work related activities during class, which may distract them and other students around them [35, 41, 71]. When students engage in risky digital behaviours at school, they may inadvertently expose their peers as well.

In this paper, we focus most of our attention on tweens — children aged 10 to 13 years — and their teachers. The technology risks not only affect tweens, but also their teachers who become primarily responsible for mitigating the risks, and providing support and guidance to tweens as they navigate digital media [6, 7, 9, 12, 28]. We explore technology risks teachers see or feel prepared to assist tweens with, including those on educational technology platforms and on personal devices used within the school setting. Teachers have become primarily responsible for proactively teaching digital literacy skills to tweens, so that these maturing children understand the rules of engagement on digital media, and know how to avoid or handle risky situations. Teachers have assumed these responsibilities because (i) it is included in the K-12 curriculum [22, 27, 52–54, 56–61] (ii) teachers use technology in the classroom and thus bear the responsibility for teaching how to safely use technology and how to properly engage in the online world.

Digital literacy represents skills children need to create and consume media; it is more than just the technical know-how, and consists of a wide variety of ethical, social and reflective practices [5, 31]. Most importantly, for the context of this paper, these include knowing how to stay safe online, protecting your personal information, and verifying the authenticity of information found online [5, 20, 31, 45]. However, many teachers report having low digital literacy skills of their own, due to lack of technology training and the fast pace of technology change, especially as it concerns usage by tweens [23, 28]. Thus, teachers might not be prepared to train tweens in this regard.

While previous research has looked at tweens' risks on digital media [6, 9, 17, 29, 36, 39, 43, 68, 76, 87, 88], few have explored them in the context of schools from the perspective of teachers [14]. We believe this is important, because teachers are primarily responsible for addressing these risks in schools and educating tweens' about safe digital behaviours. They are also in a unique position of being a significant adult figure in tweens' lives without some of the emotionally-charged dynamics that arise between tweens and their parents. Teachers also have the additional perspective of

CHI '21, May 8–13, 2021, Yokohama, Japan

ACM ISBN 978-1-4503-8096-6/21/05…$15.00
https://doi.org/10.1145/3411764.3445224

interacting with many tweens over several years, and thus are in a position to comment on trends from a first-hand observer position.

Our paper addresses this gap, and explores tweens' technology risks in schools from the perspective of teachers. We set the following three research questions for our work:

RQ1: What *issues* are teachers seeing around tweens' use of digital media?

RQ2: What *strategies* are teachers using to help tweens deal with issues involving digital media?

RQ3: How *prepared* are teachers to help tweens with these issues?

To address these research questions, we conducted semi-structured interviews with 21 Canadian elementary school teachers, who had experience in teaching digital or media literacy to tweens. Our results show that teachers are responsible for addressing a range of issues relating to digital media, the majority of which are security and privacy risks. Many of the issues they addressed originated outside of school, and continued into the school, requiring teachers to step in and help tweens resolve them. Despite these responsibilities, teachers had not received any training from school boards on how to help tweens deal with these issues. They discussed several proactive and reactive strategies for mitigating tweens' risks on digital media, and reported learning many of them on the job. We discuss the implications of our findings on how elementary schools address digital security and privacy.

2 BACKGROUND

2.1 Psychosocial development

Children experience the most significant developmental changes to their social, cognitive, and physical abilities during adolescence, which takes place between the ages of 10–19 years [49, 72]. Around this time, children also begin to use social media, and more technology with less supervision both at home and school [38, 39, 76]. Our work focuses on tweens (10–13 year olds), because it is during this time when children first begin to experience more online risks [8]. We note several psychosocial characteristics of tweens to help contextualize their risky technology-related behaviours. First, peer relationships become extremely important as part of their identity development, where opinions of friends are valued over those of their family [83]. They are more sensitive to criticism by peers, and try to fit into their peer groups [72, 83]. Tweens are also learning socially acceptable behaviours by pushing the boundaries of those behaviours, and begin to explore their sexuality [73]. It is important to note that while they are going through this development, their social, cognitive, and psychological skills are still developing, which factor into how they engage with digital media, and how they experience the associated risks.

2.2 Online risks

Much research has been done on the types of risks children experience on digital media [6, 9, 17, 29, 36, 39, 43, 68, 76, 85, 87, 88]. These risks include phishing, cyberbullying, exposure to age-inappropriate sexually explicit content, misinformation, and privacy violations [6, 9, 17, 29, 36, 39, 68, 76, 85, 87, 88]. These risks can lead to psychological distress in children, especially when they have not yet learned the appropriate mitigation strategies [40, 67]. Razi et al. [67] analyzed 12-17-year-old children's posts from an online peer support mental health forum and found that children received unwanted sexual content, struggled with how to turn down these requests, and advised others to avoid users who engaged in these behaviours [67]. Specific groups of children such as foster children and those who posses or desire online social capital are especially vulnerable to online risks [3, 40]. For example, Maghsoudi et al. [40] found that children with a high online social capital experienced more risks and psychological stress [40].

Studies have also explored the role of parents in addressing these risks and the associated challenges [9, 28, 34, 38, 77, 90]. For example, parents can have positive influences on children's online security and privacy behaviours, by modelling these behaviours themselves [7, 12, 34]. However, if parents do not possess appropriate cybersecurity and privacy skills, they may become fearful of the potential risks, and resort to a restrictive parenting style to mediate children's technology use [3, 7, 12, 15, 34, 38]. We note this approach is ineffective in the long term because it does not teach children critical thinking skills required to navigate the online world [7, 9, 38, 74] and can also negatively impact parent-child relationships [19], which are crucial during adolescence [49]. For example, an analysis of Google Play reviews of online safety apps written by children showed that the majority of reviewers (76%) gave the apps a low rating (single star), and found them to be overly restrictive and invasive of their privacy, thus negatively impacting relationships with their parents [19].

Most research relating to children and online risks either groups children into broad age ranges [9, 29, 39, 43, 76, 87, 88], or mostly focuses on teens' (as opposed to tweens') online risks [36, 68]. The most comprehensive work to date exploring children's online risks is *The EU Kids Online* project, which spans several European countries. Started in 2010, they conducted surveys about online habits and risks with European children aged 9–16 [39]. Using an updated survey, data collection was repeated with different samples between 2017 – 2019 [75]. From the most recent report, only 28% felt very confident in their ability to identify false information online, 25% reported having had a negative online interaction in the last year, and 23% reported being victims of an instance of cyberbullying in the last year, and 35% have been exposed to harmful content [75].

The 2015–2016 *Global Kids Online* pilot project [9] synthesises data about the internet habits of children aged 9–17, collected through different sources from several countries. In general, they find that younger children have more difficulty identifying misinformation, that many younger children were unaware of how to manage their privacy settings online, and a substantial minority of younger children had contact with unknown strangers. The report also reveals that few students had e-safety or digital literacy training at school, and therefore, most relied on peers for advice rather than teachers in these matters [9].

2.2.1 Content-contact-conduct risks (CCCR) model. Using findings from *EU Kids Online*, Hasebrink et al. [24] developed the *content-contact-conduct* model (Figure 1) to classify children's various online risks. We briefly explain this model because we use it to structure some of our findings (Section 5.1) later in the paper.

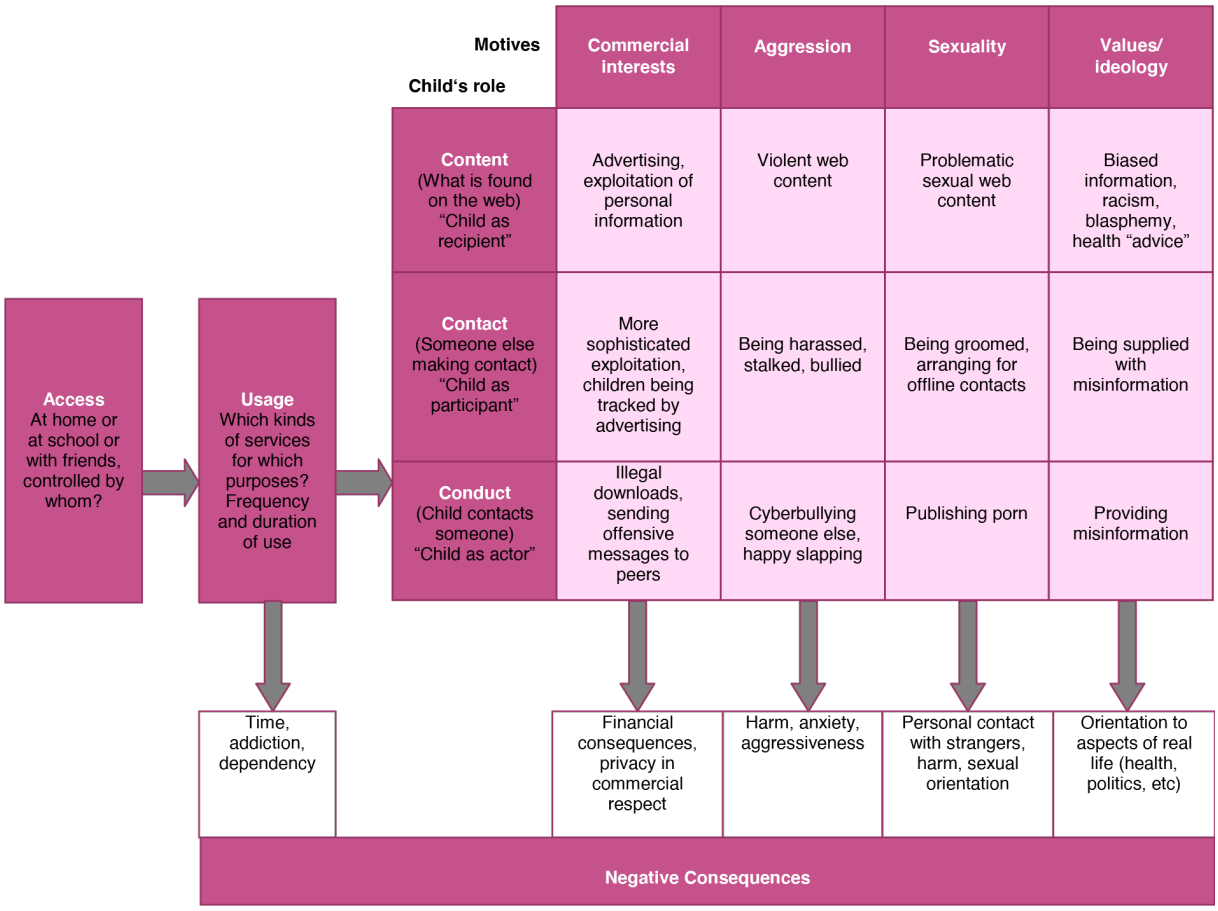

Figure 1: The content-contact-conduct risks (CCCR) model from [24].

The *CCCR* model treats risks as negative outcomes of transactions between children and online communicators, with each communicator providing content or a service to the child [24]. The model also takes into account the motivations of the communicator and role of the child during the online interaction. Communicators' motivations represented by the model include commercial interests, aggression, sexuality, and values or ideology.

Children take one of the following roles in their online communication, which exposes them to different risks when combined with motivations of the communicators:

- **Content:** child is the *recipient* of communications (example risks: advertising, misinformation)
- **Contact:** child is a *participant* in online communications (example risks: online tracking, being harassed)
- **Conduct:** child is the *actor* in online communications and initiates contact with others (example risks: sending offensive messages, cyberbullying)

A limitation of the *CCCR* model, as noted by Hasebrink et al. [24], is that sometimes the boundaries between categories are not clear, and certain risks or issues may cut across different categories (e.g., aggression and sexuality can co-occur).

2.3 Teachers

Adults, such as parents and teachers, are primarily responsible for mitigating tweens' technology risks, teaching them appropriate digital literacy skills, and providing them support so they become resilient and informed digital citizens [6, 7, 9, 12, 28]. However despite these expected roles, many teachers feel unprepared for this responsibility because they do not have the required cybersecurity knowledge or training to teach these concepts to tweens [14, 23, 28, 32, 66]. In a survey with 319 pre-service US teachers, Pusey and Sadera found that the majority had little knowledge of key cybersecurity terms such as phishing, social engineering, and bots [66]. Thus, governmental efforts at incorporating digital literacy into the curriculum will struggle with implementation, if teachers are not provided with proper training and resources.

However, very little work [14, 32] has actually looked at teachers' realities in the classroom as they relate to children's use of technology and online risks. Those that did explore this topic focused on teachers' perceptions of classroom technologies [32], and did not explore the teacher-tween relationship in terms of online risks and digital literacy education. We found only one study exploring this relationship, but in a preliminary manner. Corradini et al. [14], conducted an online survey with 2,229 Italian primary,

middle, and high school teachers to understand their perceptions of students' digital awareness. Teachers recognized the importance of improving students digital awareness, and thought that students should be taught to handle various types of technology risks such as cyberbullying, protecting personal information, and detecting misinformation. They also expressed needing training on these topics themselves [14]. However, Corradini et al.'s [14] survey did not explore teachers' perceptions in depth.

2.4 Research Gap

Our work complements the *EU Kids Online* project by exploring the risks of *Canadian tweens*, thus focusing on the unique challenges of children aged 10–13 and providing insight from a different country. In addition, we explore these risks from the teachers' perspectives, which was not covered by *EU Kids Online*. Our work also complements Corradini et al.'s [14] online survey by collecting rich qualitative data through different research methods.

3 METHODOLOGY

The study was cleared by our University's Research Ethics Board (REB). We conducted 60-minute semi-structured interviews with 21 Canadian elementary school teachers, recruited from Facebook groups, teacher blogs and websites, and posters at our university and community centres. Two pilot interviews were conducted in November 2017. Results from these were used to make significant changes to the interview script. We also expanded the recruitment method (e.g., using social media and teacher blogs), and geographic area to reach a more diverse group of teachers across Canada. We obtained REB approval for the changes, and resumed the study. The remaining 19 participants completed the study between November 2018 and September 2019. Participants were compensated with a $50 Chapters bookstore e-gift card or an email INTERAC money transfer, depending on their preference.

The interviews were conducted as part of a larger study exploring tweens' digital literacy and an educational game to teach about digital literacy. In this portion of our study, we sought to answer our three research questions.

3.1 Interviews

The interviews consisted of the following main questions. Additional probing and follow-up questions were asked as needed, depending on the responses to the main questions.

(1) What kind of issues are you seeing around tweens' media use?
(2) What types of problems are tweens bringing up in the classroom?
(3) How do tweens bring up these problems to you or another teacher?
(4) How do you (or another teacher) address these problems?
    (a) How do the parents get involved?

The interviews were completed in person or via videoconferencing, whichever was most convenient for the teachers. Interviews were audio recorded, the recordings were transcribed using the automated transcription service Trint[1], and we manually verified and corrected them as needed. We analyzed data from the final transcripts.

3.2 Participants

We recruited 21 teachers from eight different cities and four provinces across Canada, and from eighteen different schools (Table 1).

All had experience teaching grades 4-8 (M = 8 years). They had taught digital literacy to students formally as part of a course, informally through ad-hoc class discussions or integrating it with another subject. At the present, they were teaching grades 1-8. 48% (n = 10) of participants taught in private schools and 52% (n = 11) taught in public schools. Some (29%, n = 6) taught in private or public religious schools. One school followed the open-learning model, and was completely online, without a physical location. The majority of participants (86%, n = 18) were female and a few (14%, n = 3) were male, with a median age of 32 years, which is representative of this user population. All except one were employed full time at their school, and had worked there for at least 12 months. They were responsible for teaching multiple subjects, including Math, Language Arts, History, Technology, Science, Health, Religion, and Chemistry.

On average, teachers had 22 students in their classroom, with those in private schools having fewer (M = 18) than public schools (M = 25). Teachers regularly integrated technology into their classrooms, with the most common platforms being Google classroom, Chromebooks, Smartboards, and reading and math applications (e.g., Prodigy[2], Readtheory[3]). Teachers reported that their students used technology for an average of 10 hours each week for classroom activities such as taking notes, conducting research for projects, preparing presentations, collaborating with peers, and completing tests and assignments. They also used it in class to take photos, videos, and create media using software such as iMovie and GarageBand.

We used a 5-point Likert scale (1 = most negative, 5 = most positive) to capture self-reports of teachers' comfort level with technology, and their knowledge of cybersecurity and digital literacy. Most reported being very competent with technology (M = 4.52, SD = 0.51), and had moderate knowledge of cybersecurity (M = 3.52, SD = 0.60) and digital literacy issues (M = 3.67, SD = 0.58).

4 ANALYSIS PROCESS

Our approach of analyzing responses to the interview questions was inspired by the Grounded theory method as described by Strauss and Corbin [79]. Analyzing data using Grounded Theory consists of three main stages: open, axial, and selective coding. In *open coding*, data is repeatedly reviewed to create unique categories (i.e., codes) emerging from the data. The open codes are then reviewed in *axial coding* to establish relationships between them. In the final stage of *selective coding*, the codes and their relationships are used to form a broader understanding of the data [79].

As is common when working with qualitative data in HCI [48], we started our analysis after data collection was complete (i.e., we did not employ theoretical sampling). Theoretical saturation was

[1] https://trint.com

[2] https://www.prodigygame.com
[3] https://readtheory.org

Participant	Location	Experience (years)	Grades taught	School	Use of technology in classroom
p1	City 1, Alberta	1-5	6-11	Private	BYOD to record and edit videos. Chromebooks and Google classroom to collaborate.
p2	City 1 Alberta	1-5	5-11	Private	Google classroom.
p3	City 1, Ontario	16-20	2, 5-8	Public	Google classroom for research and schoolwork. Games for Language arts and Math.
p4	City 1, Ontario	6-10	4-8	Private	Google applications for research. BYOD to augment learning, and create media.
p5	City 1, Ontario	10-14	1-9	Private	Research, and practice concepts.
p6	City 1, Ontario	1-5	3-8	Private	Google classroom for schoolwork (e.g., typing). Internet safety taught using the Google curriculum.
p7	City 1, Alberta	6-10	1, 4-6	Private	Websites to augment learning (e.g., Mathletics, XtraMath, Epic!, ReadTheory).
p8	City 1, Quebec	6-10	4 and 7-11	Private	1:1 device school, where students use their devices to augment learning.
p9	City 1, Ontario	6-10	4-8	Private	Research, inspiration, and collaboration. iMovie and GarageBand to create movies, soundtracks, and commercials for Drama.
p10	City 2, Ontario	16-20	1-4, 7	Public	Research, creating presentations, listening to music, and recording media.
p11	City 1, Ontario	1-5	1-8	Public	Interactive activities, playing games, research, and accessing notes.
p12	City 3, Ontario	16-20	4-8	Public	Research, assignments (OneNote) and quizzes (Kahoot).
p13	City 1, Alberta	3	1-5	Public	Google applications for research, assignments, and collaboration.
p14	City 1, Ontario	16-20	2, 4-8	Private	Research, presentation, and creating media (e.g., iMovie).
p15	City 1, Ontario	11-15	1-7	Public	Chromebooks for taking notes, completing lessons, and collaborating.
p16	City 1, Ontario	1-5	4-5	Public	Videos, programming, practice typing.
p17	City 1, British Columbia	6-10	1-5 and 7	Private	Accessing lessons, communicating with teachers and peers, and schoolwork.
p18	City 1, Ontario	1-5	1-4 and 7-8	Public	Chromebooks for research, presentations, and creating websites.
p19	City 1, Ontario	1-5	6 and 9-12	Public	Research, assignments, and social media.
p20	City 2, Alberta	1-5	6-7 and 10	Public	Google classroom, BYOD, and Chromebooks to access homework, and complete quizzes.
p21	City 1, Ontario	16-20	4-10	Public	Google classroom, Prodigy, and EPIC.

Table 1: Participant demographic details

reached at 21 participants; we observed no new insights from the last two participants.

4.1 Application of Grounded theory approach

We printed all the transcripts, and read the first 10 to develop a sense of the data. We then read 5 of these in more detail, while annotating interesting details within the margins. In terms of granularity, we coded participants' response to each interview question, including any relevant information they provided at a later point in the interview. After annotating 5 transcripts, four top-level categories emerged from the annotated data:

Issue: the security and privacy *issues* reported by tweens,
Discovery: how teachers *discovered* these issues,
Handling: how teachers *handled* these issues,
Consequences: the potential *consequences* tweens received by the teacher and/or the school.

We used these top-level categories to organize codes emerging from the remaining 16 transcripts. Each code was written on a post-it note, and the post-it notes were organized into the four top-level categories. During the coding process, we recorded any insights or questions in the *memos* category. We reviewed the list of codes, read the transcripts again, and re-coded data or re-arranged codes within categories as necessary. In total, we created 72 codes from 420 pages of transcripts representing 26 hours of audio recorded interviews. Table 2 provides examples of how excerpts from the transcripts were coded into the four categories to address our research questions. We primarily used a paper-based process to analyze our data.

The first author conducted the interviews and was most closely engaged with the research, therefore, had the most relevant contextual experience for the analysis. Analysis was primarily conducted by this author. Intermediate results were regularly discussed with the second author to help refine the ideas and extract meaning from the data. We found it most suitable for the main researcher to primarily conduct the analysis, because the main researcher conceptualized the research, collected data, and had accumulated the necessary contextual background. Prior work [11] supports our approach, suggesting a preference for a single coder when the analysis requires an in-depth understanding of the domain, as was the case in our work.

5 RESULTS

We organize our results to specifically address each of our three research questions.

5.1 Addressing RQ1: Risks

Teachers described having witnessed various risks tweens face when using digital media, including cyberbullying, communicating with strangers online, pranks, exposure to sexual or violent content, and misinformation. Many of these risks were also identified in Hasebrink et al.'s [24] work on understanding the online risks of European children. We explore them for Canadian children, and we explore them from the unique perspective of teachers, which has not been explored before. We used Hasebrink et al.'s [24] *content-contact-conduct risks (CCCR)* model and terminology to describe our risks, and used a grounded theory inspired approach to explore each risk in depth.

5.1.1 Conduct risks. Conduct risks were the most common type of risks teachers observed among tweens. Specifically, they reported tweens participating in cyberbullying, sexting, and sharing pornography with their peers.

Cyberbullying: Teachers explained that one of the biggest problem they observed among tweens was using digital media to exchange mean messages, make fun of others, fight over friends, and participate in "drama". All these behaviours are considered cyberbullying, and can have serious consequences on the psychological and physical well-being of everyone involved [26, 62, 80, 86]. Most incidents reported by teachers happened over group chats or in private messages, since most tweens are just beginning to use more public forms of social media.

Teachers reported a spectrum of cyberbullying incidents, ranging from innocent jokes to more serious forms of harassment, such as racist comments being exchanged on social media. A teacher shared several incidents to demonstrate the range of issues she handles:

> "So, only girls involved. There was one student sending a message to two other students where they are just kind of judging them and commenting on something that they were wearing or also on one student's voice as well. Yeah, so like, *'your voice is so annoying'* or like *'why would you act this way?'* and just passing judgement and it was done through text." (p4)

At the more severe end of the spectrum, we heard about public racist comments.

> "It was two boys, and it actually became a cultural thing. [...] They were going back and forth on Instagram [making racist comments], but neither family knew that their child had Instagram." (p4)

Because this happened publicly over social media, other tweens were able to view this exchange, and brought it to the teacher's attention, who then informed the parents and the principal.

As opposed to cyberbullying with teens [88], our data suggests that most cyberbullying incidents with tweens were unintentional, where those involved did not know their behaviour was considered cyberbullying. They were trying to act cool in front of their peers, or they did not consider how others would perceive their actions.

Teachers felt that tweens need more education about cyberbullying, especially about nuanced situations which may be unclear to them. Regardless of intent, even minor cyberbullying incidents can be quite distressing to the recipient, as illustrated by an incident between two 11-year olds, which spanned several days, and made the recipient physically ill.

> "A group chat between two Grade 6 students got to a very violent level, and the little girl was throwing up every night and it was just very very scary. And when they were caught [...] the little girls bursts into tears and said *'Oh my God! I'm so happy that you found out'*. And you think 'they're 11 years old'. But you read through these text conversations and it looks like you're reading a conversation between a bunch of adults." (p14)

These tweens engaged in online behaviour that was not age-appropriate and they did not have the skills to disengage. Contrary to older teens [37], they were relieved to have adults step in to help diffuse the situation. Teachers expressed that several aspects of technology make cyberbullying worse than offline bullying. For example, since tweens have access to technology after school, cyberbullying is more persistent, as they are unable to escape it at home.

> "We are seeing that the issues coming up in person are not just ending there anymore. They can carry on because for middle school students, Grade 6,7,8, it's very common, especially in our schools, for the kids to all have cellphones. So it just doesn't stop at 3:45 when the school day ends." (p4)

When incidents take place publicly, either on social media or in group chats, anyone can participate, which can further increase the intensity of the situation. This combined with the ability to

Category	Number of Codes	RQs addressed	Example Code	Example Excerpt
Issue	35	RQ1	Exchanging mean messages	*"Lots of kids [are] commenting rude stuff. [They are] sending each other nasty texts. The biggest issue is online bullying and stuff."* (p14)
Discovery	11	RQ1	Student brought it to teacher	*"When it's gotten too far, the proof will come into the school. Sometimes there's proof, and sometimes there's not. It would be like a screenshot of Snapchat, so [it] would be a conversation. And then, when the proof has been brought forward then you can act on it in a disciplinary manner."* (p11)
Handling	15	RQ2 and RQ3	Informed the principal	*"So the group chat was sent to me. The next step is that I alert the administration right away. If there is any certain thing, at any time, that makes my spidey sense go a little bit nuts, especially since it was documented: 'he said, she said, you said, you're a b word, you are not a b word'. So, then basically it goes to the administration's hands, to be honest."* (p6)
Consequences	11	RQ2	Tech privileges revoked	*"We had a child one year who was looking up pretty inappropriate pictures of women online. So we talked with his parents, and then he was really limited in his usage at school. He was also told that if he continued he would lose the use of [his] iPad, and he would have to use a desktop computer for completing assignments which he did not want to do."* (p12)

Table 2: Example of how interview excerpts were coded to answer our research questions.

respond immediately creates an environment where issues can escalate quickly, and tweens do not have time to think things through before responding. One teacher identified this as the major issue she observed with tweens' communication over digital media.

> "I think the biggest problem is that kids are so 'in the moment' [that] they don't reflect. They react immediately without reflecting. And because it goes live and because you can't take it back, they get themselves into trouble." (p9)

In most cases, peers were the targets of tweens' cyberbullying, with those involved knowing each other in real life. We saw little evidence of tweens harassing strangers they had met solely online. In some cases, educators were the target of tweens' harassment. For example, a student frustrated with a teacher posted something negative about them on social media. While students have always expressed frustrations about their teachers, traditionally this took place in school hallways, for example. When these comments are made publicly online, they can have negative professional consequences for teachers as parents and employers may be able to access them.

Sexting and sharing pornography: Teachers described several incidents of tweens sexting or sharing pornography with their peers. For example, one teacher described an incident of a girl sending inappropriate pictures to several boys:

> "She had been sending these photos to people [...]. Like they were provocative photos. And, who knows what she was thinking when she took them. Maybe she didn't see the photos as being provocative because she sees these on covers of magazines and things like that. So then it's bringing her parents in to let them know that their daughter's doing this." (p9)

Tweens can be exposed to or share sexual content with their peers, before they are psychologically and emotionally mature to understand it. While this may also occur offline, it is less frequent, typically requires more effort, and is more challenging to share. Our teachers did describe several cases where recipients of unsolicited sexual content reported it to their parents or teachers, indicating that some tweens are comfortable discussing these issues with adults to some extent.

Teachers discussed how sexting can lead to negative long-term consequences for tweens, such as damage to their reputation, cyberbullying, and revenge porn. One teacher from a small town described an incident where a middle school girl sexted a photo to her boyfriend, who then shared it with his friends. This incident followed her through high school and into the workplace, damaging her reputation and relationships.

> "It follows them all the way through high school and they can't get away from it. The girls that I've known that have had that happen, it's hurt them forever, like all the way through their high school and they've never gotten away from it. To me that's the most harmful thing [...]. I've seen people completely socially isolate themselves, like they become an outcast. It hurts all their friendships and their potential future relationships and even employers here start hearing about that kind of stuff." (p12)

Another teacher explained her anxiety over how to handle such situations in the classroom:

> "I always try to keep it in the back of my mind, it's just like, 'how am I going to deal with it if that does come up in the discussion'. It frightens me honestly, as the teacher who is teaching digital literacy. The idea of that being a potential thing that is talked about

> in class, and the fallout from that, does weigh in the back of my mind sometimes." (p8)

5.1.2 Contact risks. Teachers described only two contact risks, where adults targeted and communicated with tweens. These included: talking to strangers online and being targeted with misinformation.

Communicating with strangers: Teachers reported instances of tweens communicating with strangers online despite knowing the risks of this behaviour in the real world, as explained by one teacher:

> "They think it's totally fine to talk to somebody on the Internet they don't know, without any research, when they're doing games or things. Although, that being said, they [either] also automatically assume that the persons are totally fine or trying to kidnap them, like there's no in-between." (p7)

Tweens communicate with strangers online primarily to socialize with people who have similar interests. This type of communication allows them to interact with and learn from diverse communities, but it may also expose them to risks that they are unprepared to handle. Thankfully, most incidents reported by our teachers were minor. However, one teacher described a high-risk incident where a girl contacted strangers on social media looking for her parent, with whom she did not have any contact:

> "I had a student, her parent was not at all involved in her life, had zero custody over [her]. She was looking for her parent on the Internet, searching her parent's name. She was messaging with people she didn't know, who were much older than her." (p6)

Detecting misinformation: Teachers reported that tweens are very susceptible to misinformation online, and often do not know how to fact-check information shared with them. Misinformation targeted at tweens often takes the form of viral challenges and hoaxes, which were described to be especially problematic by teachers. The latest significant case of misinformation they described was the *Momo challenge*, a viral internet hoax about self-harm [25, 69]. It leads people to believe that a creepy doll called Momo randomly appears in YouTube videos and encourages children to commit suicide. Teachers reported this hoax creating fear among tweens, leading them to initiate class discussions about misinformation online.

> "The Momo was a big topic for a long period of time and how kids were believing stories that were about Momo that was true or not true. Lots of kids took it very seriously and then a couple weeks later, we realized it was just a hoax. But some kids were genuinely scared." (p16)

Tweens' fear in the Momo was partially fueled by parents and other adults, who also believed the misinformation. Thus, the responsibility fell on teachers to correct the misinformation, and reassure tweens. Some teachers stated that they stay informed about dangerous viral challenges and proactively discuss them with their students, while others take a more a reactive approach, addressing issues as they come up in the classroom.

Respecting copyright: In Grades 4-6, students begin to use information from websites, blogs, and multimedia to complete their school work. However, teachers described several incidents where students plagiarized entire essays, by copying information verbatim from websites. They expressed that this primarily occurred because students did not understand copyright rules, but in some cases, they did it knowingly and hoped not to get caught.

> "They're still not fully understanding what plagiarism is. They're not really understanding that they can't just copy and paste from a site and put it in their report. So that's kind of a big challenge, teaching that and finding the resources to say how we do this." (p6)

Teachers expressed that this was an issue in older grades as well, requiring them to re-educate students throughout high school, so that they have a good understanding of it before entering university, where the consequences of plagiarism are more severe.

5.1.3 Content risks. Our teachers described three types of content risks experienced by tweens online: exposure to sexual content, aggressive content, and advertising.

Sexual content: The main content risk for tweens, as described by teachers, was exposure to unwanted sexual content. Tweens may encounter this content unintentionally, often from using problematic keywords in a search engine. For example, teachers explained that due to tweens' developing reading skills, they commonly used the image search results in search engines, which has a higher chance of showing inappropriate sexual content.

Tweens also use the internet to explore their sexuality, and may intentionally seek out sexual content. While being curious about sexual topics is a normal part of tweens' development, our data shows that searching for this information online may expose them to unwanted content and risks if they do not possess the appropriate digital literacy skills and psychological maturity. Several teachers expressed concerns over these behaviours, and described incidents where tweens looked up this type of information during class.

> "We had one child one year who was looking up like pretty inappropriate pictures of women online. [...] I think he was just doing it to be really silly and to show everyone what he could do. And then he was also told that if he continued that he would lose the use of iPad and he would have to use a desktop computer for completing assignments which he did not want to do." (p7)

When tweens look up sexual information online during class, they may inadvertently expose their peers to this information, requiring the teacher to explain it to the rest of the class. In many cases, teachers felt unprepared to have these conversations with middle school students.

Aggressive content: Although tweens are also exposed to aggressive, violent content on social media or YouTube, our teachers were most focused on multi-player games such as Roblox [13] and Fortnite [18], which are popular among tweens. Since tweens are particularly susceptible to behaviour modeling [4], teachers stated that viewing aggressive content leads some to engage in aggressive behaviours with their peers in real life or on digital platforms. This

is especially problematic on all-ages digital platforms such as multiplayer games, where tweens may learn aggressive behaviours and language from adults, and believe them to be socially acceptable. One teacher explained a situation of tweens modelling aggressive behaviours from Roblox.

> "So they see the other people doing it, and they mimic those actions, which is teaching them that it's OK to do that. And usually [they are learning from] older people because you never know who you're playing with online. [...] So I do see a lot more aggression for the kids that are playing games like that." (p13)

Advertising: Tweens often use search engines to research material for school projects. As part of this process, teachers explained that tweens often encounter advertising on websites, and are unable to differentiate between advertising and legitimate content on the website, making them unknowingly susceptible to marketing or other outside influences. One teacher described such a situation, where tweens were looking up interest rate information for a bank.

> "We have all this information coming at us that they're like, 'click on it!'. When they first saw the [advertising] pop-up, they were like 'Look what I found!' [...] They thought they searched and that's what they got as a result of the search. Kind of is, but it was aimed at them, rather than finding it." (p6)

5.2 Addressing RQ2: Mitigation strategies

5.2.1 Reactive approaches. Teachers described two main approaches they used to handle risky situations with tweens: addressing it on their own or escalating it to the principal. They explained that the approach used depended on several factors, such as the type and severity of the incident, level of exposure to other tweens, and whether it was a recurring behaviour for those involved.

> "I think it's kind of on a case by case basis, and it depends on the severity of the issue. If it's kids being mean online, it's usually [...] just a 'meet with the kids' kind of situation. So if it continues, then it will get escalated. We'll bring in the school resource officer or the school counselor more appropriately and then if it escalates, it goes to [the] admin." (p20)

Of the incidents described, teachers considered contact risks such as cyberbullying and sexting to be the most severe, because these had more severe consequences for the tweens involved. Since these incidents are also included in the Canadian Criminal Code [55], many schools involved the police if they considered a situation to be severe, in terms of the emotional, physical, and social harm to those involved.

> "[...] lingerie shots are considered pornographic. As are of course nudes. So the police have to be involved because the children are over 12 and anybody over 12 that's doing stuff like that can be actually charged under the Criminal Code. Same with the cyberbullying. They can also be charged, particularly if they use certain words. Or if it's homophobic or whatever." (p10)

These schools often had pre-existing relationships with the police, and their involvement was primarily to educate. However, when tweens showed a clear disregard for the law and repeatedly engaged in negative behaviours, they faced more severe consequences such as expulsion, and possible criminal charges.

5.2.2 Proactive approaches. To protect tweens from engaging in risky behaviours, schools monitored their use of technology, and used community learning experiences, workshops, and invited guest speakers to improve their digital literacy.

Monitoring use of technology: Some schools disallowed students from using their personal devices, in an effort to reduce technology-related distractions, and to deter tweens from participating in drama or cyberbullying at school. One teacher explained such policy at her school:

> "We're not a Bring Your Own Device (BYOD) school so that's one area that we don't really have an issue with. If they have a cell phone, it needs to be in their bag. If someone uses it in class, it gets confiscated, sent to the office, [and] you go pick it up at the end of the day. I don't like to keep it in my desk in case it does go missing [...] if I give it to the principal, it's out of my hands. And then if it gets stolen off his desk, it's not my responsibility." (p3)

Even with strict policies, teachers were responsible for monitoring students' device use and for enforcing the rules. For example, they would ban devices in certain classes (e.g., gym, drama), to prevent students from taking embarrassing photos and videos of each other, and possibly sharing them. Teachers also felt extra responsibility given that mobile devices are expensive and frequent targets for theft.

On school issued devices, some schools implemented filters to control tweens' access to websites and to monitor their online activities, while others found these limiting to tweens' intellectual development. Teachers had mixed reactions in response to these filters. Some used them to minimize distractions in class and to manage student behaviours. Others felt that the filters are not representative of the real-world, where children are able to freely explore the internet. One such teacher explained:

> "We don't have filters in the school system, because I believe the school board thinks the kids should have that freedom to do that research or to collect that information. As educators, we have to be proactive and let them know that there is no firewall or there is no protection." (p10)

The debate here revolves around whether tweens should be kept in a digital "walled garden" to protect them, or be given freedom but taught coping skills, recognizing that some mistakes will be made. Filters can also interfere with pedagogy if it impedes access to legitimate resources that the teacher wants to use (e.g., some YouTube videos are educational).

Community learning experiences: In addition to monitoring tweens' technology use, schools also made efforts to increase tweens' awareness of risky behaviours, and improve their critical thinking skills, thereby creating more empowered digital citizens. One such approach was community learning experiences, where

teachers discussed with the entire class incidents that took place within their school or that were popular in the media. After presenting an incident, teachers asked students what they would do, and then discussed possible preventative strategies. Using this approach, teachers leveraged real-life incidents as teaching moments, because they found that tweens' learned best from the experience of their peers, as they could relate to them. For example, one teacher described using this approach to discuss sexting with tweens:

> "Last year we had a student in Grade 6 sending naked pictures of herself to some boys in the school. And obviously, one of the boys finally came to a teacher and said *'hey this is going on'*. So we approached the parents [...]. We brought in a school resource officer, and had a whole kind of conference as a school, not just for this one student, but as the school, on what that can look like, what [can happen by] putting something online or putting something through an app, even an app like Snapchat that deletes it." (p20)

We note that when this approach is used, teachers must protect the privacy of all parties involved. They should also obtain permission from tweens' and their parents, to ensure they are not further harmed or triggered by reliving the incident when it is discussed broadly with the school. Although teachers did not explicitly express this as a concern, they did describe situations where students and their parents became upset when a teaching moment violated students' privacy. For example, a teacher described an online safety talk, where the speaker, a police officer, included students' social media photos in his presentation without their permission:

> "The guy that we had at the time was very upfront. We were all in the gym watching, grade 7 and 8 students, and he started showing pictures of the kids on the screen: a picture of a kid at camp, a picture of a kid from a birthday party [...]. The kids were like *'Where did you get my photo? Where did you get that?'* One of the pictures showed a boy sitting in a hot tub [...]. The kid was really embarrassed about it. [...] And the mom called the school and the community officer and was just livid and said *'How dare you show that?'* And he said *'well the ironic thing is I got that off [your/mom's] Facebook page!'*. " (p12)

Workshops: Some teachers helped create school-wide workshops to proactively address common issues. In most cases, these workshops were developed in collaboration with the school librarian, resource officer, or psychologist, who could provide students with additional support on specific topics. Teachers expressed that tweens' engaged in risky behaviours either because of low digital literacy skills, or due to their developing psychosocial and communication skills. For example, teachers stated that many cyberbullying incidents take place because of tweens' poor self-regulation and conflict resolution skills, prompting them to design workshops to address these issues:

> "We have a great school psychologist who comes in 2.5 days a week. That's part of my job too, as I am the student life coordinator. So the two of us have identified this as a need for Grade 6 around social dynamics: How do you solve social conflicts? How do you treat one another? How do you act face-to-face? How do you act online?" (p4)

When discussing how to improve tweens' psychosocial and communication skills, teachers noted that digital media has introduced new psychosocial skills for tweens. For example, many teachers expressed that tweens must now learn how to interpret and understand tone in online communications, which is difficult to do, even for adults. One teacher explained, how the absence of this skill can lead to inadvertent cases of cyberbullying:

> "Students are not reading the tone of people properly and not understanding when someone says, *'I'm trying to sleep now. You need to stop messaging me and harassing me while I'm asleep'* or *'I'm working. Like stop harassing me or bothering me while I'm working, I'm trying to get stuff done'*. And that can definitely be classified as harassment and bullying." (p8)

School resource officers (SROs) and guest speakers: Teachers also reported inviting speakers, such as cybersecurity experts and public health professionals to discuss certain digital literacy topics with tweens. These speakers usually came to the school once a year to speak to different grades, and were invited back as needed. In general, teachers liked using guest speakers, because they felt that students needed to hear online safety information from third parties, in addition to parents and teachers. As one teacher explained:

> "So hearing it from somebody else, sometimes makes a bigger impact, especially if it's somebody that they're taught to have respect for, like the police. I like that they can talk about the legal aspects, and they often give very specific local examples without naming names." (p12)

The most commonly involved third-party were school resource officers, who are police officers responsible for safety and crime prevention in schools [10]. SROs act as law enforcement, educators, and counselors in schools. Most teachers described them being used in the latter two roles. Although, if students participated in violence or illegal activities, then the SROs were involved as law enforcement. Teachers only described two such incidents. One case involved drug dealing on campus, where a group of tweens posted Snapchat videos of themselves doing drugs. In another case, a student distraught over a romantic relationship brought a knife to school with the intent to harm someone, and was discovered by teachers because she posted about it on social media beforehand. In both these cases, the students were expelled, and they faced more severe repercussions from the SROs.

Recently, the SRO program has received criticisms for increasing negative interactions between youth and police and criminalizing traditional disciplinary issues, thereby exacerbating the school-to-prison pipeline [70]. There is also evidence that these programs disproportionately affect minorities from low socioeconomic status [2, 16, 84], making these students feel anxious and less safe in schools with SROs [82]. While the majority of our participants had positive perceptions of SROs, some echoed the concerns from the literature. From a pedagogical perspective, teachers explained that SROs typically focus on threats and behaviours considered to be criminal, and some use scare tactics, which can give tweens an

exaggerated sense of possible threats. This approach can also make tweens fearful of using technology. As one teacher explained:

> "The idea can get into their heads where it's like, *'well, I went online once and then you know the scary 60 year-old guy in the woods comes along and then you're kidnapped!'* [...] It just goes from innocent chat room to kidnap [...]. 'No. Guys, like there are other issues of data sharing, privacy, things that maybe we also need to talk about before.' " (p8)

Recent criticisms of SROs, as part of larger conversations around police brutality, have prompted school boards in Canada to revisit their SRO programs, with some cancelling the programs completely due to them being problematic and ineffective [21, 50, 51]. Since many SROs were also the primary source of online safety training, their termination will leave a gap which will need to be addressed by teachers.

5.3 Addressing RQ3: Teachers' preparedness

For teachers to effectively help tweens deal with online risks, and teach them safe digital behaviours, they need to have support from their administration, appropriate training, and access to resources. We review how well our teachers were supported across these three factors.

5.3.1 Support from administration. We consider support both in terms of the resources available to teachers, and the direct assistance provided by school administration in handling risky tween behaviours.

In dealing with risky behaviours, teachers only involved principals in more serious cases of cyberbullying, sexting, distribution of pornography, violence, or illegal activities. When this happened, teachers generally found the principals to be supportive in helping them deal with these situations. In most cases, the principal took over, communicating with the parents, tweens, and other relevant parties such as the SROs or the school psychologist.

However, when it came to digital literacy education, teachers reported that administrators were reactive rather than proactive. When an incident occurred, either in the school or within the broader community, teachers were asked to discuss it with tweens. Beyond that, teachers were provided with very little direction in terms of what tweens should learn. As one teacher explained:

> "It's really sad, but the only time it ever comes up will be when something bad happens. Like, I don't know, a kid watching Netflix in class. So like email comes out and *'I need teachers to be extra vigilant. The kids are doing this in class now.'* [...] It's when there's a negative thing, it's like not [a] precaution." (p9)

This reactive approach was also largely applicable to the training and resources provided to teachers by administrators.

5.3.2 Training. Most teachers reported not receiving any pre-service or on-the-job training prior to teaching digital literacy to tweens. They reported learning to teach these topics from experience, using resources they had accumulated over time. Typically, school boards did not provide teachers with any training opportunities, and those interested had to seek them out, and complete them on their own time. This high opportunity cost of training combined with teachers' already busy schedules, makes it inaccessible to the majority, as explained by one teacher:

> "The tough part is that they're all outside of regular school hours, so you're gonna get the people who are interested and want to invest their time. But that closes doors for a lot of people who maybe would find it really useful, but can't because of personal commitments. Or by 4:30 they're exhausted and the last thing they want to do is go sit in a classroom for two hours listening to somebody else talking." (p12)

We note that our participants were highly motivated and experienced in teaching digital literacy, and while many expressed the importance of digital literacy training, only a few had voluntarily participated in training opportunities due to the high opportunity costs. Thus, those new to teaching security and privacy are less likely to have any formal training on the subject, before teaching it to tweens.

Our teachers also lacked access to informal training opportunities within their schools, such as mentorship programs between experienced and new teachers. In fact, many teachers expressed that they teach in silos, where teachers do not share resources and are unaware of each others' teaching practices, meaning that teachers do not have opportunities to learn from each other. As one teacher explained, while discussing the inclusion of digital literacy education across subjects:

> "It should be every curriculum teacher's responsibility. [...] I mean, if somebody comes in and talks to me about it, we're so segregated in silos, but if we're using these tools we need to show [students] no matter what subject we're teaching." (p5)

5.3.3 Resources. When designing their digital literacy lessons, teachers expressed that they typically use resources from their personal collection accumulated over time. Teachers who did not have these accumulated resources described the process of finding them as follows:

> "It's self-taught. So whenever I need to do a lesson, let me see what's online. I'll take a little bit from here, little bit from there and sort of morph it together and make a lesson. Teachers notoriously beg, borrow, and steal. So I mean the Internet's your best friend." (p3)

Thus, teachers used Google to search for lesson plans and activities for their targeted digital literacy topics. This, combined with the lack of training, places new teachers at a significant disadvantage. Due to these challenges, some teachers may teach these topics only at a superficial level, just to meet their curriculum requirement, as explained by one teacher when discussing the approach of her peers:

> "I need to fill in a digital literacy mark [from the curriculum]. Okay, I need them to critique this. Okay, I did one lesson, mark done, move on." (p5)

This illustrates that just because digital literacy is included in the curriculum, does not mean that tweens are actually acquiring the required competencies. In general, teachers reported that schools do not provide them with a central repository of relevant ready-to use educational resources. The exception to this were the digital

citizenship and cyberbullying resources provided by the Ontario Physical and Health Education Association (OPHEA) [63]. Despite being outdated (last updated in the late 1990s), these resources were still being used by teachers in the province of Ontario, who had positive perceptions of them.

Teachers also expressed purchasing digital literacy resources from Teachers-Pay-Teachers (TPT) [81], an international online marketplace for original classroom resources designed by teachers. As explained by one participant, teachers liked TPT because they could easily obtain resources that met their curriculum, and they were willing to pay out of their pocket for this convenience:

> "Hundreds of dollars spent on teachers-pay-teachers. Because it takes you so long to create a unit, I would rather buy a unit that someone already created for the Ontario curriculum that has all the activities and the cumulative tasks and all the information. [...] I might not teach it exactly like they lay it out, but it gives me like a framework to go off of. Because it takes days to make a unit. [...] Like there's just literally only so many hours in the day and some things are worth paying for." (p18)

Our data suggests that, overall, private school teachers seemed to have more assistance from their staff of IT professionals, psychologists, librarians, and clerics, in helping them design their digital literacy lessons. They also had memberships to certain organizations, which provided access to additional resources. For example, one teacher reported that by being a member of the International Baccalaureate Programme (IBP) [64], her school received access to resources and guides from the IBP.

6 DISCUSSION

6.1 Technology domains

The interconnectivity provided by technology has led to a shift in societal norms, where the lines between work and home are increasingly blurred [30]. Our conversations with teachers revealed that this is also happening in schools, especially those using BYOD. Specifically, we noticed that when describing issues children experienced on digital media, teachers discussed issues relating to educational technology (e.g., learning management systems, Google classroom) and children's personal devices and media (e.g., mobile device, social media) interchangeably. Similar patterns emerged in their handling of these issues in schools. Essentially, we observed that teachers did not differentiate between issues children experienced on educational technology or their personal devices and media. This could be attributed to the increased use of BYOD devices in schools and the lack of filtering on school-owned devices. For BYOD schools, teachers expressed that while it was difficult to monitor children's activities on these devices, their benefits — such as personalized learning opportunities — outweighed the risks. Teachers monitored the use of these devices in class, but children were allowed to use them unsupervised during breaks, which they acknowledged made it difficult for children to be present. Children were also more easily distracted in class when personal conversations continued over digital media while children completed school work on their devices. (e.g., social media notifications during a lesson).

Most technology risks reported by teachers concerned children's personal devices and media, and did not include the risks they face on educational platforms, such as Google classroom, which was the most common platform used in our schools. When mentioned, teachers discussed these platforms in the context of children using them to engage in risky behaviours (e.g., looking up inappropriate images on Google), and not in terms of the inherent privacy risks they pose to children. For example, teachers did not discuss how Google and Apple products (e.g., iPads) largely integrated into Canadian schools present considerable privacy concerns, such as how schools monitor children's technology use [42], and the types of data they collect and share with the technology vendors [44, 91]. With regards to monitoring tools, several teachers reported using them to monitor children's activities on school-owned devices, and perceived them as a protective mechanism for children. Those who did not use these tools or stopped using them did so because they found them to be ineffective, and not because of their privacy implications for children. We speculate that our participants' lack of discussion on the risks of educational technology could be attributed to several factors: (i) Teachers may not have an in-depth knowledge of the privacy risks posed by these technologies, which is consistent with prior work [32]. While our participants had experience teaching digital literacy, they reported having a moderate knowledge of digital literacy and cybersecurity issues, mostly learned through workshops or the media. (ii) Teachers focused on risks which affect their daily teaching life, which happened to be the risks children experience on their personal devices and social media.

6.2 Tweens: growing up digital

Most of the issues reported by teachers were the result of tweens engaging in typical tween behaviours which became risky *because they occurred over digital media*. For example, during pre-adolescence, it is normal for tweens to explore their sexuality, however when they do so over technology (e.g., searching for certain terms), it exposes them to new risks, and these normal pre-adolescent behaviours are perceived as a transgressive by the adults around them. In this sense, tweens are discovering their identifies, developing their social skills, and relationships while making mistakes along the way. However, the consequences of their mistakes are amplified, and they are making these mistakes in front of an audience, with potential long-lasting impacts due to the associated digital trail.

6.2.1 Psychosocial development with technology. We note three properties of technology that exacerbate tweens' mistakes or amplifies common behaviours on digital media: being always-connected, public, and permanent.

Always-connected: When tweens have constant access to technology, minor incidents can quickly escalate, because those involved do not get a chance to take a step back, reflect on what is happening, and respond appropriately. As their self-regulation skills are still developing [78], tweens can get easily overwhelmed by what is happening in a situation, and respond immediately without thinking of the long-term consequences or how their actions might be perceived by others. Teachers expressed this as the trigger behind the most common incidents they addressed (e.g., cyberbullying).

This need to be always connected to technology, can be partially perpetuated by FoMO (Fear of Missing Out) [65], where tweens are

afraid of missing or being left-out of social situations. Over 20% of Canadian tweens even sleep with their cellphones [76] ostensibly due to FoMO. However, in addition to being detrimental to tweens' overall well-being, being always-connected to technology can also lead to more social issues, which often overflow into school and become the responsibility of teachers. Thus, we believe that some of these issues could be reduced by parents modelling positive technology behaviours at home and establishing rules around screen time. Establishing these rules and boundaries during pre-adolescence may help children in later stages of adolescence when their lives become more complex.

Public: With technology, tweens are under constant surveillance from their peers, family, and teachers, who may broadcast their mistakes to a wider audience, either intentionally or unintentionally, without the tween's permission. In these situations, tweens never intended for their mistake or vulnerable moments to become public and when they did, tweens felt their privacy was violated, often by trusted parties. Teachers reported that many of the issues they dealt with happened because tweens did not respect each others' privacy, and these privacy violations had more severe consequences over digital media than in person. For example, in many situations tweens publicized the private photos or conversations of their peers without their permission. These incidents suggest that issues surrounding personal and social boundaries are especially problematic on digital media.

The public nature of technology may also encourage tweens to participate in more attention-seeking or status-seeking behaviours than they would under other circumstances, as they seek approval from peers and perform for a digital audience. Attention-seeking and status-seeking are normal characteristic behaviours of tween development, but these may also draw unwanted, undesirable, or dangerous attention when they take place online, including from predatory adults. For example, our teachers described a situation where a tween posted a suicidal photo on social media in a moment of frustration, due to a difficult home situation. Teachers checked in with the tween, but also had larger conversations with her about the potential consequences of these posts in terms of drawing the attention of individuals encouraging self-harm, some of which specifically target tweens.

Permanent: Tweens' behaviours on digital platforms are somewhat permanent due to the digital trail, and can follow them into adulthood. Teachers expressed this as a particular concern, explaining that tweens do not actually understand the potential long-term consequences of their actions. However, perhaps expecting tweens to understand these potential long-term consequences is unrealistic considering their developing cognitive skills and limited life experience. Instead, there needs to be a shift in social norms, where minor errors in judgement by tweens on digital media are not used as a factor in decisions that could have significant impact on their future, such as employment opportunities and college admissions. This also suggests a need for additional features on digital platforms in terms of facilitating control (or even automatic deletion) of digital trails, especially for youth.

Despite some of the negative implications of the digital trail for tweens, teachers in our study also had positive perceptions of it because it helped them discover problematic tween behaviours, so they could intervene and provide assistance. We found that teachers often encouraged tweens to take screenshots of problematic digital behaviours, and report them to a teacher or parent. Having a digital trail as evidence also helped teachers in handling these situations and deliver appropriate consequences to the tweens involved. This leads to an interesting dynamic where tweens are encouraged to capture potential *'evidence'* on one hand, but are also being taught to respect other people's privacy and to ask for consent. Thus, it may be challenging for tweens to navigate these seemingly contradictory behaviours.

6.3 Implications for teachers

6.3.1 Wide range of digital literacy skills: Teachers are required to teach a wide range of digital literacy and online security, privacy, and safety skills that cannot simply be captured in one class. These lessons instead must span multiple different subjects, ranging from Health, Language Arts, to Technology. Thus, teaching tweens digital literacy skills then becomes the responsibility of several teachers in the school, who must collaborate and engage in co-teaching activities to ensure that they adequately cover all aspects of digital literacy. Based on our conversations with teachers, this rarely happens, despite being desired. In reality, most teachers are teaching in silos, often creating their own class materials addressing topics which they consider to be most important at the time.

In addition to teaching how to use technology, teachers also need to educate tweens about new social norms that dictate the responsible use of technology in society. Teachers expressed that digital literacy education among tweens should include development of interpersonal skills, as their absence particularly exacerbates communication and interpersonal issues among tweens.

Teachers explained that teaching certain digital literacy topics was more challenging compared to others, requiring them to adopt different instructional strategies depending on the topic. They found teaching topics such as copyright to be the easiest, because the correct or incorrect choices are clear, making them easier to comprehend for children. For these topics, passive strategies were used to present the material, followed by hands-on activities to practice the learned material. However, many digital literacy topics involve nuanced situations without a clear "correct" answer, requiring teachers to encourage critical thinking skills in children. Teachers found these topics to be most challenging to teach, requiring more effort, and the use of creative experiential learning techniques. One such topic was digital citizenship, which includes teaching children good digital etiquette and social interaction strategies with others online. Given the significant cases of cyberbullying described by our participants, teachers found this to be a particularly important topic for tweens, one where they need to be taught empathy for others, to look at things from someone else's perspective, and strategies to diffuse emotionally charged situations. Given the complexities of these skills, teachers found they were best taught using experiential learning techniques, where children were provided different online situations, and the opportunity to make different choices and learn how their choices would affect others. One such technique used by teachers was role-playing, where children took on different roles to act out a situation provided by the teacher. This is an area where HCI designers, such as those in

game design and virtual reality, can help by designing experiential digital literacy activities for educators.

It is impossible, and arguably unwise, to shield tweens from all online risks. Thus, in supporting tweens through adolescence, we should instead be building their resilience, so that they are better prepared to address risks and handle any negative consequences resulting from these risks [89]. To build resilience in tweens, teachers must build rapport and create safe spaces that allow tweens to discuss their online experiences, and receive support from teachers. From a pedagogical perspective, teachers should use educational approaches that allow tweens to practice their critical thinking skills, instead of using a solely prohibitionary approach towards technology. However, from our interviews with teachers, we found that many did use prohibitionary approaches, and our data shows that this could be because they have low digital literacy skills themselves or lack the appropriate training to discuss these issues with tweens.

6.3.2 Parents as partners. Most of the issues reported by teachers originated outside of the classroom, with teachers often being notified only when the situation became severe. Given this, teachers viewed parents as having a key role in helping mitigate and prevent risky tween behaviours. Specifically, they expressed that parents should have regular conversations with tweens about positive technology behaviours, and offer support to build resilience. They also saw parents as having an active role in improving tweens' overall digital literacy. To do this, some teachers shared digital literacy resources with parents through Twitter or their teaching blogs.

However, while teachers wanted parents to be involved, they acknowledged that not all parents have the necessary digital literacy skills to do so, or that the tweens might not be comfortable openly discussing their risky digital behaviours with their parents. In these cases, teachers became the *'first responders'* to tweens' risky behaviours and their primary sources of support. To maintain positive rapport with tweens, teachers did not always notify or involve parents when tweens encountered a problematic situation on digital media. They preferred to only involve parents for more severe cases that placed the tween or others in harm.

6.4 Implications for schools

6.4.1 Provide digital literacy framework. We found that most teachers taught digital literacy haphazardly, with reactive approaches to address issues as they arose. The topics addressed were also heavily influenced by the media, and consisted of more sensationalized topics, such as online predators and the exploitation of tweens. While these topics are important, they often overshadowed other important digital literacy topics, such as as online tracking and data privacy.

We also found inconsistency in terms of how digital literacy was addressed by different schools, even those within the same school board. Thus, we believe that schools would benefit from a digital literacy framework to provide teachers with more direction and guidance in terms of how to teach digital literacy skills competencies as laid out in the curriculum. Addressing this need in Canada, we note efforts towards the creation of the *USE, UNDERSTAND & CREATE* framework by MediaSmarts — a not-for-profit organization that promotes digital and media literacy in Canadian homes and schools. This comprehensive framework provides teachers with advice on how to integrate digital literacy in K-12 [46]. While this framework has been available since 2015, our conversations with teachers suggest that more effort needs to be invested in promoting and implementing it in individual schools and school districts.

Schools should also provide teachers with empirically validated tools and resources for teaching digital literacy. Many of our teachers reported finding the resources they used online, buying them from Teachers-Pay-Teachers (TPT), or having accumulated them over time from their experiences of teaching digital literacy. This may lead them to take a prohibitionary approach towards teaching digital literacy, or skip teaching it altogether due to the effort required. It may also lead to teaching outdated material or ineffective practices as technology evolves.

6.4.2 Support training. Our teachers highlighted that one challenge to teaching digital literacy was the lack of pre-service and on-the-job training available. Thus, schools need to facilitate digital literacy training opportunities, and support teachers' efforts to participate in training. Due to the constant evolution of technology and their risks, it is not sufficient for schools to train teachers only once; teacher knowledge and skills need regular updates. One potentially feasible approach for schools is to establish mentorship or train-the-trainer programs between less experienced and more experienced teachers. Our teachers were enthusiastic about these informal approaches, and being able to share their experiences with others. One teacher in our study was participating in a digital literacy program between different schools in her district, and expressed how she enjoyed sharing teaching strategies and resources with other teachers, and learning from their experiences.

7 LIMITATIONS AND FUTURE WORK

We note several limitations of our study. The first relates to the recruitment of our participants. While we made an effort to recruit teachers from different provinces across Canada, the majority were from a single city in Ontario, and generally employed in schools located in areas of medium to high socioeconomic status. We also note that a disproportionate number of participants taught at private schools. Due to the difficulty in recruiting teachers who met the eligibility criteria for our study, we were unable to control for socioeconomic status and type of school.

As we recruited teachers who were experienced and interested in teaching digital literacy, it is possible that we would get different results from those who are less experienced. Future studies should recruit teachers from schools in different socioeconomic status communities to collect a more representative sample of the user population. Less experienced teachers in teaching digital literacy should also be recruited. Although our sample was representative of the teacher population in terms of gender, it would also be interesting to recruit a sufficient sample to compare whether approaches differed depending on the gender of the teacher.

7.1 Researcher profile

The researcher who coded the data and conducted the analysis has a background in HCI and Computer Science, with expertise in usable security. Having taught undergraduate HCI and Computer Science courses, the researcher is familiar with doing qualitative

analysis, including using Grounded Theory. The researcher was primarily home-schooled, so does not have personal classroom experiences of being a tween and interacting with teachers. The researcher's background may have unintentionally influenced the analysis, however, the researcher tried to remain objective and did not do the analysis with a pre-conceived theoretical model or understanding.

8 CONCLUSION

As tweens begin to use more technology for school, and to socialize and develop relationships, they also encounter more risks. During this critical period of development, tweens need support from their teachers in dealing with risky situations and to learn the appropriate digital literacy skills. However, despite these expectations, little is known about teachers' lived classroom experiences and challenges in helping tweens in this regard. To address this, we conducted semi-structured interviews with 21 Canadian elementary school teachers to understand the risks teachers witness tweens facing on digital media, teachers' mitigation strategies, and how prepared teachers are to help tweens. We used grounded theory to analyze our results, which showed that teachers mitigate a variety of risks for tweens, ranging from minor privacy violations to more severe cases of physical and psychological harm. Most issues reported by teachers were the result of typical tween behaviours which became risky because they took place over digital media. We provide some implications of these results on teachers and schools. Specifically, teachers need to address a wide range of digital literacy skills to ensure that tweens are adequately equipped for the digital world. In addition, parents and teachers need to work together as a partnership in this effort. To ensure that teachers can help tweens, schools need to support teacher training, and provide them with more direction in terms of how digital literacy should be addressed in schools.

9 ACKNOWLEDGMENTS

We thank the participants for their time, and the reviewers for their feedback in improving the paper. We also acknowledge research funding from the Ontario Early Researcher Award and the Canada Research Chairs program.

REFERENCES

[1] Oluwaseun Akeju, Sergey Butakov, and Shaun Aghili. 2018. Main factors and good practices for managing BYOD and IoT risks in a K-12 environment. *International Journal of Internet of Things and Cyber-Assurance* 1, 1 (2018), 22–39.

[2] Yolanda Anyon, Jeffrey M Jenson, Inna Altschul, Jordan Farrar, Jeanette McQueen, Eldridge Greer, Barbara Downing, and John Simmons. 2014. The persistent effect of race and the promise of alternatives to suspension in school discipline outcomes. *Children and Youth Services Review* 44 (2014), 379–386.

[3] Karla Badillo-Urquiola, Xinru Page, and Pamela J Wisniewski. 2019. Risk vs. Restriction: The Tension between Providing a Sense of Normalcy and Keeping Foster Teens Safe Online. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'19)*. ACM, New York, NY, USA, 1–14. https://doi.org/10.1145/3290605.3300497

[4] Albert Bandura and Richard H Walters. 1977. *Social learning theory*. Prentice-hall, Englewood Cliffs, NJ, USA.

[5] David Bawden. 2008. Origins and concepts of digital literacy. In *Digital literacies: Concepts, policies and practices*, Colin Lankshear and Michele Knobel (Eds.). Peter Lang Publishing, New York, NY, USA, 17–32.

[6] Ilene R Berson and Michael J Berson. 2006. Children and Their Digital Dossiers: Lessons in Privacy Rights in the Digital Age. *International Journal of Social Education* 21, 1 (2006), 135–147.

[7] Kara Brisson-Boivin. 2018. *The Digital Well-Being of Canadian Families*. MediaSmarts. Retrieved June 20, 2020 from https://mediasmarts.ca/sites/mediasmarts/files/publication-report/full/digital-canadian-families.pdf

[8] Pedro Quelhas Brito. 2012. Tweens' characterization of digital technologies. *Computers & Education* 59, 2 (2012), 580–593.

[9] Jasmina Byrne, Daniel Kardefelt-Winther, Sonia Livingstone, and Mariya Stoilova. 2016. *Global Kids Online Research Synthesis, 2015-2016*. UNICEF Office of Research Innocenti and London School of Economics and Political Science. Retrieved January 10, 2021 from https://www.unicef-irc.org/publications/pdf/IRR_2016_01.pdf

[10] Public Safety Canada. 2018. School Resource Officer (SRO) Program. Retrieved September 10, 2020 from https://www.publicsafety.gc.ca/cnt/cntrng-crm/crm-prvntn/nvntr/dtls-en.aspx?i=10152

[11] Kathy Charmaz. 2014. *Constructing grounded theory*. Sage Publishing, Thousand Oaks, CA, USA.

[12] Stephane Chaudron, Rosanna Di Gioia, and Mônica Gemo. 2018. *Young children (0-8) and digital technology, a qualitative study across Europe*. Publications Office of the European Union. https://doi.org/10.2760/294383

[13] Roblox Corporation. 2006. Roblox Login Page. Retrieved September 10, 2020 from https://www.roblox.com

[14] Isabella Corradini and Enrico Nardelli. 2020. Developing digital awareness at school: a fundamental step for cybersecurity education. In *Proccedings of the International Conference on Applied Human Factors and Ergonomics (AHFE'20)*. Springer, Berlin, Germany, 102–110. https://doi.org/10.1007/978-3-030-52581-1_14

[15] Lorrie Faith Cranor, Adam L. Durity, Abigail Marsh, and Blase Ur. 2014. Parents' and Teens' Perspectives on Privacy in a Technology-Filled World. In *USENIX Conference on Usable Privacy and Security (SOUPS '14)*. USENIX Association, California, USA, 19–35.

[16] Tony Fabelo, Michael D Thompson, Martha Plotkin, Dottie Carmichael, Miner P Marchbanks, and Eric A Booth. 2011. *Breaking School Rules: A Statewide Study of How School Discipline Relates to Students' Success and Juvenile Justice Involvement*. New York Council of State Governments Justice Center. Retrieved September 10, 2020 from https://knowledgecenter.csg.org/kc/system/files/Breaking_School_Rules.pdf

[17] Organisation for Economic Co-operation and Development (OECD). 2011. *The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them*. OECD Publishing. Retrieved September 10, 2020 from https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf

[18] Epic Games. 2017. Fortnite – A Battle Royale Game. Retrieved September 10, 2020 from https://www.epicgames.com/fortnite

[19] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J LaViola Jr, and Pamela J Wisniewski. 2018. Safety vs. surveillance: what children have to say about mobile apps for parental control. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'18)*. ACM, New York, NY, USA, 1–14.

[20] Google and iKeepSafe. 2018. K-12 Digital Citizenship Curriculum. Retrieved June 20, 2020 from https://beinternetawesome.withgoogle.com/en_us/resources

[21] Andrea Gordon. 2017. *TDSB votes down police presence in high schools*. Toronto Star. Retrieved September 10, 2020 from https://www.thestar.com/yourtoronto/education/2017/11/22/tdsb-votes-down-police-presence-in-high-schools.html

[22] Academica group. 2019. New project focused on improving digital literacy, curriculum kicks off in NWT. Retrieved June 10, 2020 from https://www.academica.ca/indigenous/new-project-focused-improving-digital-literacy-curriculum-kicks-nwt

[23] Anna Gruszczynska and Richard Pountney. 2013. Developing the concept of Digital Literacy in the context of Schools and Teacher Education. *Enhancing Learning in the Social Sciences* 5, 1 (2013), 25–36.

[24] Uwe Hasebrink, Sonia Livingstone, Leslie Haddon, and Kjartan Olafsson. 2009. *Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online*. London School of Economics and EU Kids Online. Retrieved September 10, 2020 from http://eprints.lse.ac.uk/24368/1/D3.2_Report-Cross_national_comparisons-2nd-edition.pdf

[25] John Herrman. 2019. Momo Is as Real as We've Made Her. Retrieved September 10, 2020 from https://www.nytimes.com/2019/03/02/style/momo-mania-hoax.html

[26] Sameer Hinduja and Justin W Patchin. 2010. Bullying, Cyberbullying, and Suicide. *Archives of suicide research* 14, 3 (2010), 206–221. https://doi.org/10.1080/13811118.2010.494133

[27] Michael Hoechsmann and Helen DeWaard. 2015. Mapping digital literacy policy and practice in the Canadian education landscape. Retrieved September 10, 2020 from https://mediasmarts.ca/teacher-resources/digital-literacy-framework/mapping-digital-literacy-policy-practice-canadian-education-landscape.

[28] Annalise Huynh and Nisa Malli. 2018. *Levelling Up: The Quest for Digital Literacy*. Brookfield Institute for Innovation Entrepreneurship. Retrieved September 10, 2020 from https://brookfieldinstitute.ca/levelling-up

[29] Lisa M Jones, Kimberly J Mitchell, and David Finkelhor. 2012. Trends in Youth Internet Victimization: Findings From Three Youth Internet Safety Surveys 2000–2010. *Journal of Adolescent Health* 50, 2 (2012), 179–186.

[30] Sebastian Köffer, Lea Anlauf, Kevin Ortbach, and Björn Niehaves. 2015. The Intensified Blurring of Boundaries Between Work and Private Life through IT Consumerisation. In *European Conference on Information Systems (ECIS'15)*. AIS, Atlanta, GA, USA, 1–17.

[31] Tibor Koltay. 2011. The media and the literacies: media literacy, information literacy, digital literacy. *Media, Culture & Society* 33, 2 (2011), 211–221.

[32] Priya C Kumar, Marshini Chetty, Tamara L Clegg, and Jessica Vitak. 2019. Privacy and Security Considerations For Digital Technology Use in Elementary Schools. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'19)*. ACM, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300537

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

[34] Kristiina Kumpulainen and Julia Gillen. 2020. Young Children's Digital Literacy Practices in the Home. In *The Routledge Handbook of Digital Literacies in Early Childhood*, Ola Erstad, Rosie Flewitt, Bettina Kümmerling-Meibauer, and Íris Susana Pires Pereira (Eds.). Routledge, New York, NY, USA, 93–108.

[35] Kumar Laxman and Craig Holt. 2017. Bring your own device or bring your own distraction. *International Journal on E-Learning* 16, 3 (2017), 245–263.

[36] Amanda Lenhart. 2009. *Teens and Sexting*. Pew Research Center, Washington, DC, USA. Retrieved January 10, 2021 from https://www.pewresearch.org/internet/2009/12/15/teens-and-sexting

[37] Sonia Livingstone. 2014. Developing social media literacy: How children learn to interpret risky opportunities on social network sites. *Communications: The European Journal of Communication Research* 39, 3 (2014), 283–303. https://doi.org/10.1515/commun-2014-0113

[38] Sonia Livingstone and Jasmina Byrne. 2018. Parenting in the Digital Age. In *Digital Parenting: The Challenges for Families in the Digital Age*, Giovanna Mascheroni, Cristina Ponte, and Ana Jorge (Eds.). The International Clearinghouse on Children, Youth and Media, New York, NY, USA.

[39] Sonia Livingstone, Leslie Haddon, Anke Görzig, and Kjartan Ólafsson. 2011. *Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries*. EU Kids Online. Retrieved January 10, 2021 from http://eprints.lse.ac.uk/33731

[40] Rose Maghsoudi, Jennifer Shapka, and Pamela Wisniewski. 2020. Examining how online risk exposure and online social capital influence adolescent psychological stress. *Computers in Human Behavior* 113 (2020), 106488.

[41] Bernard R McCoy. 2016. *Digital distractions in the classroom phase II: Student classroom use of digital devices for non-class related purposes*. University of Nebraska - Lincoln. Retrieved January 10, 2021 from https://digitalcommons.unl.edu/journalismfacpub/90

[42] Danielle McLaughlin. 2017. *Schools Don't Need Cellphone Search Policies. They Already Have The Charter*. The Huffington Post. Retrieved January 6, 2021 from https://www.huffingtonpost.ca/danielle-s-mclaughlin/schools-dont-need-cellphone-search-policies-they-already-have-the-charter_a_23275824

[43] Samuel McQuade and Neel Sampat. 2008. *Survey of Internet and At-risk Behaviors*. Rochester Institute of Technology. Retrieved January 10, 2021 from https://scholarworks.rit.edu/article/142

[44] Common Sense Media. 2019. State of EdTech Privacy Report. Retrieved January 6, 2021 from https://privacy.commonsense.org/resource/2019-state-of-edtech-privacy-report

[45] MediaSmarts. 2012. Digital and Media Literacy Outcomes by Province and Territory. Retrieved September 10, 2020 from http://mediasmarts.ca/teacher-resources/digital-and-media-literacy-outcomes-province-territory

[46] MediaSmarts. 2015. USE, UNDERSTAND & CREATE: A Digital Literacy Framework for Canadian Schools. Retrieved January 20, 2017 from http://mediasmarts.ca/teacher-resources/use-understand-create-digital-literacy-framework-canadian-schools

[47] Keith W Miller, Jeffrey Voas, and George F Hurlburt. 2012. BYOD: Security and Privacy Considerations. *IT Professional* 14, 5 (2012), 53–55.

[48] Michael J Muller and Sandra Kogan. 2010. *Grounded theory method in HCI and CSCW*. Cambridge: IBM Center for Social Software.

[49] National Academies of Sciences, Engineering, and Medicine. 2019. *The Promise of Adolescence: Realizing Opportunity for All Youth*. National Academies Press, Washington, DC. https://doi.org/10.17226/25388

[50] CBC News. 2020. University of Alberta research to take nationwide perspective on school resource officer program. Retrieved September 10, 2020 from https://www.cbc.ca/news/canada/edmonton/u-of-a-research-to-take-nationwide-perspective-on-school-resource-officer-program-1.5716345

[51] CBC Kids News. 2020. Hamilton kids celebrate no more police in their schools. Retrieved September 10, 2020 from https://www.cbc.ca/kidsnews/post/hamilton-kids-celebrate-no-more-police-in-their-schools

[52] Government of Alberta. 2017. Information and Communication Technology Curriculum - Grades 1-12. Retrieved September 10, 2020 from https://education.alberta.ca/media/3114953/ictpos.pdf

[53] Government of British Columbia. 2017. Applied Design, Skills, and Technologies Curriculum - Grades 1-12. Retrieved September 10, 2020 from https://curriculum.gov.bc.ca/curriculum/adst/6/core

[54] Ministry of Education. 2012. The Ontario Curriculum - Grades 1-12. Retrieved September 14, 2020 from http://www.edu.gov.on.ca/eng/teachers/curriculum.html

[55] Department of Justice. 2019. Criminal Code (R.S.C., 1985, c. C-46). Retrieved May 11, 2020 from https://laws-lois.justice.gc.ca/eng/acts/c-46/section-163.1.html

[56] Government of Manitoba. 2012. Literacy with Information and Communication Technology Curriculum - Grades 1-12. Retrieved September 10, 2020 from http://www.edu.gov.mb.ca/k12/tech/lict/index.html

[57] Province of New Brunswick. 2017. Unleashing the power of literacy New Brunswick's Comprehensive Literacy Strategy. Retrieved January 10, 2021 from https://www2.gnb.ca/content/dam/gnb/Departments/petl-epft/PDF/Literacy/Unleashing_the_power_of_literacy.pdf

[58] Government of Nova Scotia. 2016. Nova Scotia's Action Plan for Education. Retrieved June 10, 2020 from https://www.ednet.ns.ca/education-actionplan

[59] Government of Prince Edward Island. 2009. Prince Edward Island Senior High Curriculum. Retrieved June 10, 2020 from http://www.gov.pe.ca/photos/original/edu_cmp52109.pdf

[60] Government of Saskatchewan. 2012. Technology in Education Framework. Retrieved September 10, 2020 from http://publications.gov.sk.ca/documents/11/85655-Technology-in-Education-Framework.pdf

[61] Government of Yukon. 2018. Digital Literacy and Citizenship for Yukon Students and Teachers. Retrieved June 10, 2020 from https://yukondigitalcitizen.ca

[62] Justin W Patchin and Sameer Hinduja. 2006. Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying. *Youth Violence and Juvenile Justice* 4, 2 (2006), 148–169. https://doi.org/10.1177/1541204006286288

[63] Ontario Physical and Health Education Association (OPHEA). 1995. OPHEA Teaching Tools. Retrieved June 20, 2020 from https://www.ophea.net/teaching-tools

[64] International Baccalaureate Program. 1995. About page of the International Baccalaureate Program. Retrieved September 10, 2020 from https://www.ibo.org

[65] Andrew K Przybylski, Kou Murayama, Cody R DeHaan, and Valerie Gladwell. 2013. Motivational, Emotional, and Behavioral Correlates of Fear of Missing Out. *Computers in Human Behavior* 29, 4 (2013), 1841–1848. https://doi.org/10.1016/j.chb.2013.02.014

[66] Portia Pusey and William A Sadera. 2011. Cyberethics, Cybersafety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference. *Journal of Digital Learning in Teacher Education* 28, 2 (2011), 82–85. https://doi.org/10.1080/21532974.2011.10784684

[67] Afsaneh Razi, Karla Badillo-Urquiola, and Pamela J Wisniewski. 2020. Let's Talk about Sext: How Adolescents Seek Support and Advice about Their Online Sexual Experiences. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'20)*. ACM, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376400

[68] Victoria Rideout and Micheal B Robb. 2018. *Social Media, Social Life: Teens Reveal Their Experiences*. Common Sense Media.

[69] Andy Robertson. 2019. *Don't Panic, What Parents Really Need To Know About 'Momo Challenge'*. Forbes. Retrieved July 30, 2020 from https://www.forbes.com/sites/andyrobertson/2019/02/27/dont-panic-what-parents-really-need-to-know-about-momo-challenge

[70] Joseph B Ryan, Antonis Katsiyannis, Jennifer M Counts, and Jill C Shelnut. 2018. The Growing Concerns Regarding School Resource Officers. *Intervention in School and Clinic* 53, 3 (2018), 188–192. https://doi.org/10.1177/1053451217702108

[71] Mukesh Kumar Saini and Neeraj Goel. 2019. How Smart Are Smart Classrooms? A Review of Smart Classroom Technologies. *ACM Computing Surveys (CSUR)* 52, 6 (2019), 1–28. https://doi.org/10.1145/3365757

[72] Renata Arrington Sanders. 2013. Adolescent Psychosocial, Social, and Cognitive Development. *Pediatrics in Review* 34, 8 (2013), 354–8. https://doi.org/10.1542/pir.34-8-354

[73] Peter Scales, Arturo Sesma, and Brent Bolstrom. 2004. *Coming into Their Own (How Developmental Assets Promote Positive Growth in Middle Childhood)*. Search Institute Press, Minneapolis, MN.

[74] Wonsun Shin, Jisu Huh, and Ronald J Faber. 2012. Tweens' Online Privacy Risks and the Role of Parental Mediation. *Journal of Broadcasting & Electronic Media* 56, 4 (2012), 632–649. https://doi.org/10.1080/08838151.2012.732135

[75] David Smahel, Hana MacHackova, Giovanna Mascheroni, Lenka Dedkova, Elisabeth Staksrud, Kjartan Olafsson, Sonia Livingstone, and Uwe Hasebrink. 2020. *EU Kids Online 2020: Survey results from 19 countries*. EU Kids Online. Retrieved January 10, 2021 from https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf

[76] Valerie Steeves. 2014. *Young Canadians in a Wired World, Phase III: Life Online*. MediaSmarts. Retrieved January 10, 2021 from https://mediasmarts.ca/ycww/life-online

[77] Valerie Steeves and Cheryl Webster. 2008. Closing the Barn Door: The Effect of Parental Supervision on Canadian Children's Online Privacy. *Bulletin of Science, Technology & Society* 28, 1 (2008), 4–19. https://doi.org/10.1177/0270467607311488

[78] Laurence Steinberg, Grace Icenogle, Elizabeth P Shulman, Kaitlyn Breiner, Jason Chein, Dario Bacchini, Lei Chang, Nandita Chaudhary, Laura Di Giunta, Kenneth A Dodge, et al. 2018. Around the world, adolescence is a time of heightened sensation seeking and immature self-regulation. *Developmental Science* 21, 2 (2018), 1–13. https://doi.org/10.1111/desc.12532

[79] Anselm Strauss and Juliet Corbin. 1994. Grounded Theory Methodology: An Overview. In *Handbook of Qualitative Research*, Norman K Denzin and Yvonna S Lincoln (Eds.). Vol. 17. Sage Publications, Thousand Oaks, CA, USA, 273–285.

[80] Paris S Strom and Robert D Strom. 2006. Cyberbullying by Adolescents: A Preliminary Assessment. *The Educational Forum* 70 (2006), 21–36. https://doi.org/10.1080/00131720508984869

[81] Teachers Pay Teachers. 2006. Teaching Resources and Lesson Plans. Retrieved September 10, 2020 from https://www.teacherspayteachers.com

[82] Matthew T Theriot and John G Orme. 2016. School Resource Officers and Students' Feelings of Safety at School. *Youth Violence and Juvenile Justice* 14, 2 (2016), 130–146. https://doi.org/10.1177/1541204014564472

[83] Hershel D Thornburg. 1980. Early Adolescents: Their Developmental Characteristics. *The High School Journal* 63, 6 (1980), 215–222.

[84] Lisa H Thurau and Johanna Wald. 2009. Controlling Partners: When Law Enforcement Meets Discipline in Public Schools. *New York Law School Law Review* 54 (2009), 977–1020.

[85] Sreenivas Sremath Tirumala, Abdolhossein Sarrafzadeh, and Paul Pang. 2016. A survey on Internet usage and cybersecurity awareness in students. In *Proceedings of the Conference on Privacy, Security and Trust (PST'16)*. IEEE, New York, NY, USA, 223–228. https://doi.org/10.1109/PST.2016.7906931

[86] Robert S Tokunaga. 2010. Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior* 26, 3 (2010), 277–287. https://doi.org/10.1016/j.chb.2009.11.014

[87] Patti M Valkenburg and Jochen Peter. 2011. Online communication among adolescents: An integrated model of its attraction, opportunities, and risks. *Journal of Adolescent Health* 48, 2 (2011), 121–127. https://doi.org/10.1016/j.jadohealth.2010.08.020

[88] Marco Flavio Michele Vismara, Joseph Toaff, Giuliana Pulvirenti, Chiara Settanni, Emma Colao, Serena Marianna Lavano, Riccardo Cemicetti, David Cotugno, Giuseppe Perrotti, Viviana Meschesi, et al. 2017. Internet Use and Access, Behavior, Cyberbullying, and Grooming: Results of an Investigative Whole City Survey of Adolescents. *Interactive Journal of Medical Research* 6, 2 (2017), 1–24. https://doi.org/10.2196/ijmr.6231

[89] Pamela Wisniewski, Haiyan Jia, Na Wang, Saijing Zheng, Heng Xu, Mary Beth Rosson, and John M Carroll. 2015. Resilience Mitigates the Negative Effects of Adolescent Internet Addiction and Online Risk Exposure. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'15)*. ACM, New York, NY, USA, 4029–4038. https://doi.org/10.1145/2702123.2702240

[90] Seounmi Youn. 2008. Parental Influence and Teens' Attitude toward Online Privacy Protection. *Journal of Consumer Affairs* 42, 3 (2008), 362–388. https://doi.org/10.1111/j.1745-6606.2008.00113.x

[91] Elana Zeide. 2018. Education Technology and Student Privacy. In *The Cambridge Handbook of Consumer Privacy*, Evan Selinger, Jules Polonetsky, and Omer Ten (Eds.). Cambridge University Press, Cambridge, UK, 70–84.