Law enforcement, justice circles, educators and parents, among others, commonly express concerns over youth welfare online (Fisk 2016; Hinduja and Patchin 2014; Livingstone and Sefton-Green 2016). The seemingly ‘limitless victimization risk’ (Hinduja and Patchin 2009, 24) online is referred to as ‘cyber-risk’ (Adorjan and Ricciardelli 2019a). In this paper, we focus on student perspectives of school-based responses to cyber-risk. Cyber-safety programs and initiatives often address cyber-risks such as cyberbullying and sexting, including the especially aggravated cases of ‘revenge porn’, and tend to target female teens (Grenoble 2012; Poltash 2013). While cyberbullying regularly occurs outside of school, it is often tied to incidents that start at school, with impacts that resonate within the spatial and temporal boundaries of school (e.g., Roher 2012; Tokunaga 2010). Fisk (2016) refers to this overlap as the blurring of lines that school administrators must manage (see also Livingstone and Sefton-Green 2016). Although researchers have found that many students have no direct experience with cyberbullying, sexting or related victimization (Lenhart 2009; Mitchell et al. 2012), such actions impact the student body as a whole, indirectly affecting students, and the school’s (offline) environment (Shariff and Gouin 2006; Stewart and Fritsch 2011).

Early researchers interested in cyberbullying (starting around the mid-2000s) usually focused on the etiological factors that influence students to engage in cyberbullying, as well as questions of prevalence, victimization, and the connections between offline and online bullying (e.g., Campbell 2005; Shariff and Gouin 2006; see also Hinduja and Patchin 2014 for a meta-analysis of extant research on cyberbullying). Efforts to advance this body of work shifted in the 2010s to program evaluations designed to address cyberbullying in schools. Cassidy and her colleagues (2013, 587), for example, argue that ‘beyond merely teaching about cyberbullying, the curriculum should focus
on empowering students in terms of digital literacy, technological skills, critical thinking skills, netiquette, e-safety, assessing their own online risks, measures to protect themselves, their reputation, and their privacy online.’

One recent systematic review evaluating randomized control trials assessing school responses to bullying and cyberbullying similarly found that most studies did not indicate positive effects long term. However, a ‘whole school’ approach was found to be more effective in ameliorating bullying behaviors (Cantone et al. 2015). This approach seeks to prevent issues of cyber-risk (whether from cyberbullying, sexting, or otherwise) from exacerbating among students, conceiving intervention along multiple dimensions and including the entire school community in the process (Tangen and Campbell 2010). While studies into the whole school approach indicated mixed results, with ‘very few programs achieving a reduction of [bullying] near or above the 50% mark,’ (Tangen and Campbell 2010, 226), it is often viewed as the optimal direction for schools to proceed in effectively tackling cyber-risk and safety (Pearce et al. 2011).

Nonetheless, despite some evidence of successful programs, a number of challenges have also been identified through this research. For instance, researchers have found a ‘differing commitment of school staff’ towards programs (Van Ouytsel, Walrave, and Van Gool 2014, 208). Others examining student perceptions about cyberbullying found that, from student standpoints, neither teachers nor parents were able to effectively assist with cyberbullying (Mark and Ratcliffe 2011). This, Limber and her colleagues (2004, 66) suggest, may relate to

a lack of concern regarding problems of bullying at their school (and within society at large), a lack of time and energy on [the] part of already-stressed staff, and/or a lack of comfort with or understanding of [the] particular model. (quoted in Van Ouytsel, Walrave, and Van Gool 2014, 208)

Similar findings were reported by Cassidy (2012) and her colleagues. They found that although Canadian secondary school educators advocated for preventative approaches to cyberbullying and prioritized digital citizenship around technology use, the schools and the school board in their study did not have ‘a specific cyberbullying policy; instead educators were supposed to follow the district’s [existing] bullying policy’ (Cassidy, Brown, and Jackson 2012, 526–527).1 Moreover, while this research involved students, educators did not express interest in learning what these students had to say about cyberbullying, thus this social problem was left ‘under the radar’. Johnson (2015, 354) points out in his study on digital literacy and citizenship among female youth that ‘digital skills are only available to students whose teachers have a special interest in the subject or to students who have the interest and agency to ask for them.’ As such, digital skills are not common curriculum in the schools and instead exposure to such information is very much tied to who teaches which students as well as presentations from external authorities. Researching school cyber-safety responses directed at students in grades 6–12 across six school districts in the United States, Fisk (2016) found a lack of emphasis on dialogue and open communication with students. Schools, instead, relied on presentations from police and IT professionals but nothing else in terms of other programs or curriculum (Fisk 2016).

An emerging body of researchers address a remaining lacuna in knowledge: how the students themselves perceive school approaches to addressing cyber-risk. Fisk (2016, 149), for instance, draws critical attention to

the lack of salience that Internet safety concepts hold for both young people and adults in everyday life. The typologies and languages of youth Internet safety do not sync with the ways that young people explain their concerns and experiences with the Internet.

Our own research with Canadian teens found that students often dismiss or do not identify with words such as ‘cyberbullying’, especially male students who may disassociate themselves from the highly gendered messages (e.g., females may be shamed while males idealized when sexting) around the possible negative consequences tied to ‘sexting’ (boyd 2014; Ricciardelli and Adorjan 2018; Vandebosch and Van Cleemput 2008; Walton 2005). Perhaps this is one reason that, addressing
Canadian students, Steeves (2010, 6) and her colleagues critique cyber-safety campaigns as ‘ineffective because they focus on dangers that are both highly unlikely and at odds with young people’s social experiences.’

Student reception of cyber-safety programs and initiatives is an emerging area of research, in part because the various cyber-risks are rapidly evolving with technological developments (e.g., concerns over teen sexting have more recently become associated with their use of the application Snapchat (Handyside and Ringrose 2017; Poltash 2013). Fisk (2016, 161) found students largely supported efforts by schools to promote cyber-safety, but thought of their efforts as simply promoting ‘common sense’ and not ‘being stupid.’ The most frequently raised criticisms were related to school curricula being deemed outdated, providing too much ‘generic information’, and emphasizing ‘extreme cases’ which were unconvincing and not relevant to the students’ daily experiences (Fisk 2016, 163). Notably, however, Fisk (2016) reports that younger students found the programs and responses more relevant than older students. Summing up his findings, he states ‘put simply, middle school and high school students are tired of youth internet safety’ (Fisk 2016, 166). Thus, it appears that the challenge plaguing schools and youth is not necessarily if they are receiving messages, but more about the messages being received, specifically their applicability and students’ ability to relate to and apply such messages in their day-to-day experiences.

**Current study**

In the current study, we aim to add qualitative details to inform understandings of student reception to school cyber-safety programs. Drawing on data collected through focus groups with Canadian teens, we, first, highlight youth criticisms of cyber-safety programs, including that students often cannot relate to the programs due to their presentation of information considered stereotypical or less relevant to the everyday realities students face online. We underscore trends according to gender and age, and then turn to student reflections on receiving only minimal, perfunctory messages about cyber-risk by the time they reach high school. These trends suggest an implicit expectation that students embrace and internalize a prudent sense of self-discipline and responsibilization.

**Methods**

We conducted focus groups with teens to explore their attitudes and experiences online, here centering on their responses towards school policies and responses to cyber-risk. Researchers drawing on focus group research to examine youth and cyber-risk are relatively rare compared with larger-scale quantitative research on cyberbullying (e.g., Agatston, Kowalski, and Limber 2007; Allen 2012; Lenhart 2009; Vandebosch and Van Cleemput 2008). Our aim is to unpack the ‘situated character’ of experience within the ‘practical and mundane contexts’ of people’s everyday lives (Sparks, Girling, and Loader 2001, 888; see also Stewart, Shamdasani, and Rook 2007). Doing so provides knowledge which may be geared to advancing educational policies and practices related to addressing cyber-risks among students.

**Participant sample and recruitment**

We employed a purposive, snowball sampling design, whereby initial contacts in various sectors such as schools and universities helped provide references to additional participants. In total, we conducted 35 focus groups with 115 participants aged 13–19 (average age of 15), with an average number of 3.3 participants per group (a minimum of two and maximum of five). Although we aimed for groups with no less than four participants, this was not always possible, and thus a few groups were more akin to small group discussions than focus groups. Each discussion lasted between 30 and 120 minutes and were conducted by both authors as well as select trained research assistants. Participants were referred through participating schools in both Western and Eastern Canada, specifically urban
Western and rural Atlantic regions. Both public and private schools participated in the project. School districts were approached for ethics approval after receiving university ethics approval. After school board approvals were received, school principals were contacted and with their permission focus group arrangements were made with students. Other participants were either university undergraduate students or the children of parents attending classes in university. Throughout this article we will refer to the Western, urban locations as Cyber City, and the rural, Atlantic locations as Cyberville (the collapse of multiple locations into these two pseudo-regions ensure the anonymity of participants while facilitating thematic comparisons of the data). A total of 15 groups were conducted in Cyber City; the remaining 20 groups were conducted in Cyberville. A total of 67 females and 48 males participated in our study. While our sample included some ethnic minorities, the majority of participants were White. SES is difficult to unpack given youth perceptions of family income make be inaccurate, moreover, costs of living varies tremendously between urban and rural (even remote) locations. Nevertheless, based loosely on school district, most participants in Cyber City were middle to upper middle class, and those from Cyberville from low to middle class backgrounds. Most groups were held with youth of the same gender and age/grade levels, a sampling stratification strategy designed to help ensure participants interacted with others that they would not perceive as threatening and with whom their experience may also resonate (Morgan 1997).

Data analysis

The transcribed focus group data was analyzed using an inductive, comparative approach without initially arriving at any definitive, substantive or theoretical conclusions about what the data reflected sociologically (Strauss and Corbin 1990). Concepts and theories emerged through the dynamic interaction of participants. Using NVivo qualitative analysis software, initially all mentions of a particular topic/theme within a session were noted (i.e., captured as ‘nodes’ and reported as ‘references’ in NVivo), allowing for comparison across sessions (Morgan 1997). Using NVivo, prominent themes emerged through the tracking of coding ‘nodes’ both across and within groups. Regular research meetings between the investigators ensured that thematic development emerged in a consistent and reliable manner, and helped to ensure a hermeneutically attuned validity of the data (Twinn 1998).

Results

Students in focus group discussions of school cyber-safety programs were more often negative than positive about program effectiveness. Discussions did not reveal any patterns by age, although gendered patterns did emerge. Overall, male students made fewer references to school program effectiveness. Only four such references were given by males, for instance, versus 35 references for females. Meanwhile, the majority of references by female participants (26) indicate that school programs are not effective, versus nine youth who expressed positive views about the programs. We organize the results to first present the views of students about the effectiveness of these programs, including the reasons for positive followed by the negative views. Next, we explore the intersectionality of age and gender in messages about cyber-safety and unpack our concept of the assumption of a prudent self. We conclude by presenting the lessons youth feel they are taught in school on online safety versus the lessons they would be interested in learning but are not taught in school in the area.

Views of school cyber-safety programs

Positive views: repetition of messages and ‘creepy’ videos

Although in the minority, some of our participants expressed positive views of school-based cyber-safety programs. One group of four females from Cyber City, all aged 15, recalled receiving a
strengths-based program called ‘Cyber Pigs’ in elementary school, that encouraged student resiliency and agency (see http://mediasmarts.ca/game/cybersense-and-nonsense-second-adventure-three-cyberpigs). Fatima explains that ‘they made us do it multiple times, they did it every single year for like a really long time.’ Lexi adds: ‘yeah, and we still remember to this day, so it has to be effective somehow.’ The marked benefit of this program, put forth by Fatima and Lexi from their group, came from repetition.

Participants who expressed positive views of school-based cyber-safety programs did so often with sympathy for educators’ motivation to ensure the safety and security of their students. Some students in Cyber City referred positively to a life skills course, as expressed by Madison (16): ‘they kind of like told us how social media can help and everything so and how it can help you and also destroy what you are trying to achieve.’ Madison adds the caveat that ‘at first it’s kind of like cheesy’, but she has come to appreciate that the program is geared to help students consider the future consequences of their actions online. Other participants were supportive of videos pitched to students in junior high that incorporated some element of fear to instill a resonant message, however the caveat seems to be that the efficacy of such fear-based tactics is short-lived. This became evident in a co-ed group of three university undergraduate students in Cyber City, all aged 19. Reid, a male student, recalls watching ‘creepy videos that tried to scare kids’ in junior high, especially one video of a female student who ‘puts the picture on the wall and she rips it off [Emily in the group responds – “I remember that”], and it keeps [reappearing], you can’t like get rid of the picture, she keeps ripping it off.’ Reid argues that in showing this video, the school is aiming to convey to students ‘about when you post something on the internet, it never really disappears.’ Emily agrees ‘that was really effective.’ Asked why, she says the video is ‘something relatable, being like “oh my gosh.”’ Referring to the suicide of Amanda Todd in British Columbia as the time when she recalled seeing those videos in school, a third member of the group, Eleanor, agrees that such videos ‘got the point across pretty well, like no one was posting like anything for like a month.’ It is clear that even with the passage of time, for these undergraduate students seeing online safety videos that had a fear-inducing component served to effectively instill in students awareness of privacy and privacy management online. However, Eleanor’s comment also implies that the emotional impact of such messages may be relatively fleeting (lasting about a month).

Participants who felt cyber-safety posters are ineffective pointed to the diminishing returns of having the same posters with repetitive messages up on school walls. Judy, aged 15 from Cyber City, remarked that her school would set up ‘thousands of posters on the wall’ related to cyberbullying, but only ‘some’ students would ‘read them,’ and only ‘when they’re really bored.’ ‘Nobody really reads them because they’re the same every day, all year, and like we see them everywhere,’ adds Saylee, aged 16 from the same group. Neither posters nor cyber-safety programs were seen as providing useful, applicable knowledge. Fernando, aged 19 from Cyberville, argues that online safety talks may be ‘educational, but it was more, didn’t teach us how to do it [e.g., being safe and secure online], just talks about [it].’ A revealing exchange regarding the effectiveness of school-based cyber-safety programs occurred in a smaller group of two 19-year-old male students and part-time workers from Cyberville, Donald and David. Asked if they recalled any of the messages received in their school about online safety, both remembered school posters and assemblies about cyberbullying, though they cast doubt on the effectiveness of the assemblies in particular. David explains:

They’d have this assembly about cyberbullying, … I don’t know for me, it was a free afternoon, you know what I mean, I probably wouldn’t show up anyway, so I [am] just being honest 100 percent I’m not going to lie.

Donald does not contradict David’s remark, but offers that ‘probably a lot of the people that were affected by cyberbullying attended.’ David agrees: ‘yeah, and it probably did help some people, the people that actually went, but like I had a, I’m not going, I’m not going to cyber[bully], I never would, I never did go cyberbully someone right.’ David and Donald’s qualified approval of cyber-safety presentations, that it is likely effective for those who attend the assemblies, raises the problem of student participation in online safety school assemblies in general, but also illuminates
a related problem, namely that some students may perceive such assemblies as specifically geared only for those who have been victimized by cyberbullying rather than a problem facing the school community as a whole.

Considering the general trends in research indicating most students have not encountered cyberbullying directly (Hinduja and Patchin 2014), such assemblies, especially among students in high school, are likely to be perceived as irrelevant or at least not pertinent to them. Students may also be reticent to attend programs and initiatives with the focus on ‘cyberbullying’, a term students may not identify with (see Authors 2019a Forthcoming; boyd 2014). Thus it may be useful to cater such assemblies with wider goals of community building, communication among peers and how students can provide help to each other when dealing with online interactions more widely (boyd 2014; Walton 2005).

Critiquing non-relatable messages

A prominent theme from our discussions with youth was their inability to relate to the messages they received about cyber-risk and safety. Instead, they felt the messages were token and not relevant, especially in relation to their experiences and concerns. Frederick, age 18 from Cyber City, suggests anyone giving cyber-safety talks needs to make the content more relatable and be more knowledgeable about youth experiences online:

I think they need to be more relatable, I think that’s the issue with everything with schools try to teach us, beside actual school stuff, is it’s not really relatable, so it doesn’t really seem like they’re that knowledgeable about that sometimes. … Just some random person coming in and giving up this stuff on the PowerPoint, no one’s going to pay attention to that. It’s not really engaging.

As evidenced from Frederick’s remarks, to be convincing, what any person is teaching about cyber-risk and online safety needs to be applicable and thus ‘relatable’. Moreover, presenters need to appear informed rather than appear to just follow a predetermined script. Participants who feel school-based cyber-safety programs are not effective point to the challenges of reaching dismissive teens, especially in middle school, a challenge that only intensifies if the person presenting the information is not relatable or appears ignorant about the nuances of youth online experiences. A presenter would be more likely to catch the attention of the most dismissive youth if the lessons presented resonate with the youth’s needs and experiences. If this is not that case, as Ashley, age 13 from Cyber City states, ‘it’s hard to tell someone to like “oh, here pay attention because it’s super important” when they just don’t care.’ To be convincing then, the subject matter needs also to be in line with youth experiences, presented in a way that youth can understand the commonalities between the information and their experiences and, as we stress, come from someone youth are more likely to be able to relate to or who has real-world experience rather than a central figure of authority.

Our participants also abjured predictable and stereotypical messages that detract from more practical and applicable information. William, age 17 from Cyber City, makes this point:

If there’s someone who is going to come in, I would hope that there would be somebody who knows what they’re talking about, who can give insightful advice as opposed to kind of the blanket statements of ‘watch out for predators online’, cuz that’s not helpful at all. Like, even just examples of how conversation routes go, sort of thing, that sort of stuff, is much more helpful than: ‘oh be careful cuz predators exist, here’s a sticker [for] on your backpack’.

In line with William’s remarks, other participants expressed skepticism about the value of ‘a sticker on your backpack’ in keeping youth safe online, as well as directives not to engage in certain practices that are part and parcel of being online. For instance, Frederick argued ‘you can’t just be like; “ok don’t add people randomly”’. Well, you’re going to add people, that’s what happens on the internet.’ Also in Frederick’s group, William pointed to certain scenarios presented to students in junior high school that do not accord with the practical problems students do encounter on a regular basis. He critiqued, for example, warnings not to talk to strangers online, ‘oh this girl talked to this person [online] and then they showed up at their volleyball game and that was one of the talks we got at
our school.’ He says that while such scenarios are ‘important to kind of get across, those aren’t the sort of things’ that are most concerning, raising other problems such as ‘Instagram money flipping scams, … Facebook password resets’ and ‘more general things [like] teaching [youth] about how … hacking works and those sort of things, because those are actual threats that are common.’ He elaborates with further examples of malware, and ransomware, arguing that many students are unable to distinguish between fake and real versions of ransomware. Listing these problems, which he perceives as much more directly relevant to student safety online, he dismisses programs focusing solely on the message that ‘there’s going to be predators’ online. Related criticisms were also expressed regarding school-based sanctions for cyberbullying that are vague and do not communicate effectively to students the particular criminal code violations that are relevant to an incident. Abigail, a 19-year-old undergraduate student from Cyber City, argued that high school students ‘should be knowledgeable on what exactly [cyberbullying] is, so that you can say, what you’re doing is considered verbal assault, … I think they should be able to easily say, that what you’re doing is a crime.’

Perhaps this lack of information about the online world being taught in schools is a result of difficulties in having informed persons available to teach such materials (Johnson 2015). Other groups also dismissed cyber-safety programs in junior high for focusing too much on stereotypical risks such as when ‘a random person is talking to you’ online, and not addressing salient issues such as ‘sexting’, which was ‘never addressed’ (Fiona, 18, Cyber City; see also (Adorjan and Ricciardelli, 2019b)). It is clear from our discussions with students that they seek relatable messages that go beyond ‘stranger danger’, offering important information such as the management of privacy, risks related to hacking, and how to address relational aggression in relation to ‘sexting’, among others. They also desire clarity about how cyberbullying, sexting and related cyber-risks may constitute potential violations of the Canadian Criminal Code.

As an exemplar of an approach to cyber-safety talks that teens may prefer, Anna, a 19-year-old undergraduate from Cyber City, recalled her father, who works in the Information Technology industry, volunteering to come to her high school to speak to students about privacy and social media. Specifically, her father discussed Facebook, ‘about how your Facebook privacy settings mean nothing’. A male student in the class, however, openly expressed skepticism: ‘and then one kid in the class during this presentation was like, oh well I have this setting where you can’t even search me … I’m super protected.’ Anna goes on to recall that, with this student’s permission, her father was able to rapidly ‘hack’ the student’s phone: ‘and my dad actually was able not only [to] find him, but log into his account.’ This experience reinforced for Anna – and likely the other student – to be ‘more careful’ about social media use; ‘cuz if he [her father] can get into it, so can a random stranger I’m talking to.’

Age, and the assumption of a prudent self: ‘just assumed you knew’

As we previously noted, according to our participants’, school-based cyber-safety programs appear concentrated in elementary and junior high school. Specifically, cyber-safety programs, talks from police officers, and other initiatives become far less frequent by the beginning of high school; as William puts it, ‘they were basically non-existent for high school’. Judy offers a commonly expressed experience:

in high school [there were] not as [many cyber-safety talks] as we did in junior high school, because in junior high school it’ll happen like every month. We haven’t had one in high school yet, but [in junior high] we … mostly every month or every week we had one … now it’s barely there in high school.

Cyberville residents shared this experience. Overall, by high school, one group suggests, programs for online risk exist for students to sign up for voluntarily, but some may not be able to do so based on scheduling issues, or may not be aware of them at all.

By high school the message projected to students, based on an arguably stark decrease in the frequency of cyber-risk presentations and programs, is that students are expected to have successfully
internalized the messages instilled in programs while they were younger. Averie, age 15 from Cyber City, questions this approach with students who may not have been receptive to those earlier initiatives:

I wouldn’t mind if they brought [cyber-safety programs] in again, maybe every once in a while, because there’s some kids, like yeah they learned it when they’re young but now they kind of don’t care anymore, so it’s nice to reinforce it every once in a while.

However, the intermittent, ‘every once in a while’ model for high school programming is also questioned by some who have graduated from high school, reflecting on their experiences. Abigail recalls attending numerous high schools where a perfunctory talk on online safety is provided at the beginning of the academic year, but then not followed through:

I went to four high schools, each and every single one, at the beginning of the semester or the year, they would have a talk about how to conduct yourself online, and they would give you resources to go to if you felt you were being cyberbullied or what have you, but they never really hammered it in. They would tell you at the beginning of the year and you’d like be yeah, yeah it’s fine, and they put, uh, like a resource in your agenda that you got at the beginning of the year. … They don’t do it because they need to, and they don’t feel like they have to like, reinforce it. They’re like ‘ok, don’t be mean to each other online, don’t swear, this is the proper way to use this, this and this’ … so I found with high school and elementary school that they didn’t really care about that so much; they were more concerned with, either physical bullying or just acts that they could see.

Exacerbating this negative view of perfunctory talks, some of our participants, unfortunately, felt that school employees are more worried about reputation than instilling a safe and secure environment. These participants suggest schools may even come to ignore problems related to cyber-risk in order to protect their image and reputation. This point is raised by Helen, remarking ‘they don’t really take [bullying] as serious as they should, or they’re caring more about the school’s reputation than they are the kid, so they’re like, there’s no bullying here, we’re a great school.’ In another group of three females from Cyber City, aged 16 and 17, Mya discloses ‘I’ve heard of teacher’s kind of, and schools just brushing off the problem [of bullying] as if it’s nothing, so I think sometimes they could probably take problems more seriously.’

Relatedly, some of our participants expressed concern over the approachability of teachers and counselors, fearing that they may be identified as a peer as a ‘snitch’ (Saylee) Janiya, an 18-year-old undergraduate student from Cyber City, spoke of her ‘big fear’ approaching both teachers and counselors with a personal issue related to relational aggression online, and fearing ‘they will inevitably tell someone else’ such as a parent. She says

… there needs to be like a strict thing, like where if [students are] coming to you to talk about a cyberbullying issue, that’s what you’re talking about, you’re not going to call the mom after and let her know, it doesn’t matter the age.

Janiya is asked what she would recommend if students have particularly serious circumstances obliging the school to report, such as disclosing criminal harassment. She agrees, but remains adamant that student privacy must be protected in the more routine experiences of relational aggression students’ experience:

Yeah that level, like if you’re going to kill yourself there’s, that’s a different level, but if someone’s just like, this person made me really upset, what should I do about it, like cuz then when it’s brought up to the parents and then the parents call the school, and the school ends up getting the person in trouble and they’ll make your life worse, it’s gotta just stay confidential.

As evinced here, if youth fail to see genuine concern at the school about online experiences with real repercussions, their interest in listening to such lessons or turning to school officers for support is increasingly nullified. By high school, in sum, there exists an implicit assumption that students have successfully internalized the messages of cyber-safety instilled in earlier programming; that they have become prudent, responsible citizens. As Yasmin says, ‘I don’t think there was anything
mentioned [about cyber-risks] in high school, at least not to my recollection that would say anything about that. It was just assumed you knew’ [Authors 2019a forthcoming, p. 104, added emphasis].

Nonetheless, recognizing their remains a lacuna in effective cyber-risk programming, at least from the perspective of the students in our sample, our participants offered information about what messages about online safety should be learned in schools. Christine, a 19-year-old undergraduate student, responds by referring to the broader issue of internet addiction: ‘teaching people what’s a healthy amount of time on social media, what’s a non-healthy like, if you can’t go a day without your phone, without checking social media … maybe you need to back off a bit.’ As Christine suggests, learning how to manage time online and how to take breaks from being online are lessons that she feels need to taught; lessons that would be relevant to students and applicable in their day-to-day lives as many feel they spend excessive amounts of time online daily. Relatedly, in a group of males Reid, also 19 from Cyber City, suggests that programs such as CALM (Career And Life Management), which are offered ‘in high school’, would be also useful for younger students: ‘like those things [CALM teaches], but for more junior high focused on like internet safety.’ Reid further suggests that wider skills-based programs would also be well suited for younger students. This view – that cyber-safety programs must start at a young age far before students reach junior high school – was echoed in several discussions. For example, Christine argues cyber-safety messages have to begin at a young age because if they don’t know about the potential like, it could be like ‘oh my friend’s just being mean to me’, but if they don’t [know] how to define that, then I don’t think we’re doing a right job.

In the same group, Abigail adds:

I think what you need to do is to implement [online safety programs] at the youngest age possible … you don’t see that becoming reinforced or policed until high school. You need to start doing that at the youngest age possible so that, like you know that 1 plus 1 is 2, you’ll know that doing that kind of activity will result in severe consequences.

A different point regarding messages about privacy is expressed by William, reflecting the theme of relevant messages:

They need to start teaching the actual like, not just saying things like ‘your Snapchats are never really gone forever’ because most people will just say it deletes every 10 seconds so. I think actually telling people ‘no it’s not actually deleted, it’s saved to a server’ … like the reality of it doesn’t kick in until you give them the real information.

Thus, the central messages that our participants felt should be taught in school are about the consequences of being online (including the permanence of their digital footprint, how social media sites function and save user information), and how to recognize if a student is becoming dependent on social network sites. These issues, which appear much more mundane and less dramatic in comparison to serious incidents of cyberbullying, sexting and other such possible scandals, nevertheless address concerns teens have that, while not necessarily more important than the ‘big risks’ that are usually the focus of school programing, are often neglected.

Discussion

While previous researchers have frequently highlighted student animosity and resistance towards school-based programing related to cyber-risk and safety, our focus group discussions with teenagers aged 13–19 reveal qualitative details regarding why antagonism exists in response to certain features of such programs. We reveal some trends related to both gender and age, specifically the intersection of age and gender as the targets of cyber-safety messages in school appear to be female teens in middle school or junior high. Moreover, very few of our participants expressed positive views of programs, though when asked why they held favorable views, it became apparent that as teens grow older they may become jaded and dismissive towards certain strengths-based programs like...
‘Cyber Pigs’. Some participants further argued that younger students would benefit from repeated messages that they may come to internalize.

Criticisms most often centered on the questionable relatability of the messages. Relying on stereotypical fear-based tactics such as focusing on the dangers of online predators or advice such as not adding ‘strangers’ to one’s friend list are not entirely dismissed as irrelevant, but participants suggested complementing or even foregrounding these messages with more practical and useful information about privacy management, for instance how to keep their information safe on newer or popular applications, particularly as privacy settings tend to change or update over time.

That far more female participants expressed antagonism towards cyber-risk programs may aptly indicate the relative intensity of the messages of responsibilization they receive compared with male students. In related research, our group discussions revealed that at least some participants felt that messages of being ‘cyber prudent’ are directed more at female students than males (see Authors, 2019b forthcoming). This is based on both the content of the messages and the frequency and duration of the presentations themselves. Regarding content, female participants expressed that messages to not distribute one’s nudes often imply females should not distribute pictures of themselves for male consumption and potential non-consensual redistribution. The onus was felt to be placed on the female student, with messages implying that males are not wholly or in part responsible for their negative actions (see Authors, 2019b forthcoming).

It may be that our relatively small sample – geared for providing rich qualitative detail – may sacrifice knowledge regarding the wider patterning of cyber-safety programs in Canada as a whole. That said, previous research establishes that female students are often provided with messages reinforcing the moral weight of their online decisions; far more than male students (Karaian2014; Ringrose et al. 2013). As our focus here is student attitudes and perceptions, further research is required to address the wider question of school policies, programs and ‘best practices’, especially considering the perspectives of educators as well as parents and other stakeholders such as non-governmental organizations developing cyber-safety initiatives for youth. Quantitative assessments with larger representative samples of students would also add important knowledge regarding implementation patterns and policies in schools as well as student responses to cyber-risk programing.

An influential critique of schools as sites of both power and surveillance is advanced by Giroux (2003, 554), who argues that, in the wider context of moral panics over youth violence in the US, youth have been engendered a ‘generation of suspects.’ More recently, Fisk’s (2016, 78–79) research in US schools reveals that parents attending school talks about cyber-risk from police and IT professionals presented students as ‘inherently untrustworthy and suspicious’, drawing on a discourse of naïveté (one presenter declared ‘kids only think they know what they’re doing’). Running alongside these authoritarian tendencies is a concern among many schools for their legal responsibilities and culpability regarding incidents of cyberbullying; namely a ‘fear of litigation and lack of knowledge about the complexities of bullying – particularly cyber-bullying’, related to ‘a lack of clarity about the legal boundaries of their responsibilities to students’ (Shariff and Gouin 2006, 31–32). This fact was not lost among our participants, who often felt that schools were more concerned about their reputations or legal sanctions than the online experiences of students and prevention of harm. It is important for schools to establish clear policies and best practices for students regarding internet access (including through school computers and their own private cell phones), and related codes of conduct (Shariff and Gouin 2006).

Researchers, we advocate, need to work with school personnel toward solving a seemingly impossible problem: finding ways to connect with youth and help those who feel most vulnerable in the school environment. There may be truth in arguments for student naïveté regarding cyber-risk and going online, and their penchant to dismiss the messages they receive from adults. Nevertheless, it is important to proceed proactively, with respect for youth cultures, to send messages which are relatable but not embarrassing or patronizing. Speaking of cyberbullying and other forms of cyber-risk, Cassidy and her colleagues (2013, 596) noted that the challenge remains moving away from viewing cyberbullying ‘as a child-problem or a school-problem to a community-problem.’
This is, of course, difficult in wider neoliberal contexts where emphasis is placed upon the ideal ‘prudential citizen’ is acutely honed to calculate ongoing dangers and avoid risk (Rose 1996a, 1996b). It may thus appear ‘natural’ for schools to internalize, especially by the time they reach high school, a strong sense of individual self-responsibility towards online risk and potential harm (cf. Brenner, Peck, and Theodore 2010; Kelly and Caputo 2011). One promising direction mentioned above is the ‘whole school’ approach (Cantone et al. 2015; Pearce et al. 2011), especially those which embrace restorative or relational justice approaches, ‘cyber kindness’ initiatives, prevention and resilience (Campbell 2005; Cassidy, Brown, and Jackson 2012). Including the perspectives of students themselves is essential to moving such initiatives forward in feasible and effective ways.

Notes
1. Due to time and budgetary constraints, the present study does not aim to triangulate findings with further interviews with educators nor parents. We are presently undergoing such a project in the same jurisdictions where we interviewed teens for our previous project. Preliminary data suggests that at least among some school boards the various approaches teachers take to technology in the classroom, including cyber-safety talks, relies upon direction from the particular school’s administration (i.e., in the absence of board-level direction), and individual teacher discretion.
2. For further methodological details please see Authors (2019a Forthcoming).
3. Although we were unable to locate the original link to this video, it is still available for viewing on YouTube, under the title ‘Once you post it, you lose [sic] control over it’: https://www.youtube.com/watch?v=UmijKUwAswY
4. Our participants also discussed their experiences with messages about sexting being concentrated in middle school (i.e., junior high school). By high school these messages were less proactively presented than reactive; i.e., talks in response to incidents of non-consensual redistribution of nudes (see Authors, 2019b Forthcoming).

Disclosure statement
No potential conflict of interest was reported by the authors.

Funding
This research was funded by an Insight Development Grant from the Social Sciences and Humanities Research Council of Canada: Grant # 430-2015-00157.

Notes on contributors
Michael Adorjan is an Associate Professor in the Department of Sociology at the University of Calgary, and Fellow with the Centre for Criminology, University of Hong Kong. His research and teaching focus on youth crime and cyber-risk, fear of crime, and perceptions of police. His research appears in British Journal of Criminology, Theoretical Criminology, The Sociological Quarterly, Journal of Contemporary Ethnography and The Prison Journal.

Rosemary Ricciardelli is a Professor and the Coordinator of Criminology in the Department of Sociology at Memorial University of Newfoundland. She is an Associate Director of the Canadian Institute for Public Safety Research and Treatment (CIPSRT), where she leads the community and institutional corrections research sector, and a Senior Research Fellow with Correctional Services Canada. Her research appears in British Journal of Criminology, Sex Roles, Journal of Criminology and Criminal Justice, Canadian Review of Sociology and Theoretical Criminology.

ORCID
Michael Adorjan http://orcid.org/0000-0002-1900-2087
Rosemary Ricciardelli http://orcid.org/0000-0002-0905-8968
References

Adorjan, Michael, and Ricciardelli. 2019b. “Youth responses to the surveillance school: The bifurcation of antagonism and confidence in surveillance among teenaged students.” Forthcoming in Young.

Agatston, Patricia, Robin Kowalski, and Susan Limber. 2007. “Students’ Perspectives on Cyber Bullying.” Journal of Adolescent Health 41 (6): SS9–S60.

Allen, Kathleen. 2012. “Off the Radar and Ubiquitous: Text Messaging and Its Relationship to ‘Drama’ and Cyberbullying in an Affluent, Academically Rigorous US High School.” Journal of Youth Studies 15 (1): 99–117.

boyd, danah. 2014. “It’s Complicated: The social lives of networked teens.” London: Yale University Press.

Brenner, Neil, Jamie Peck, and Nik Theodore. 2010. “Variegated Neoliberalization: Geographies, Modalities, Pathways.” Global Networks 10 (2): 182–222.

Campbell, Marilyn. 2005. “Cyber Bullying: An Old Problem in a New Guise?” Journal of Psychologists and Counsellors in Schools 15 (1): 68–76.

Cantone, Elisa, Anna Piras, Marcello Vellante, Antonello Preti, Sigrun Danielsdóttir, Ernesto D’Aloja, Sigita Lesinskiene, Mathlias Angermeyer, Mauro Carta, and Dinesh Bhugra. 2015. “Interventions on Bullying and Cyberbullying in Schools: A Systematic Review.” Clinical Practice and Epidemiology in Mental Health: CP and EmH 11 (Suppl 1: M4): 58–612.

Fisk, Nathan. 2016. Framing Internet Safety: The Governance of Youth Online. Cambridge: The MIT Press.

Giroux, Henry. 2003. “Racial Injustice and Disposable Youth in an Age of Zero Tolerance.” International Journal of Qualitative Studies in Education 16 (4): 553–565.

Grenoble, Ryan. 2012. “Amanda Todd: Bullied Canadian Teen Commits Suicide after Prolonged Battle Online and in School.” Huffington Post [Online]. November 10. Accessed June 2018. http://www.huffingtonpost.ca/entry/amanda-todd-suicide-bullying_n_1959909.

Handyside, Sarah, and Jessica Ringrose. 2017. “Snapchat Memory and Youth Digital Sexual Cultures: Mediated Temporality, Duration, and Affect.” Journal of Gender Studies 26 (3): 347–360.

Hinduja, Sameer, and Justin Patchin. 2009. Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying. Thousand Oaks, CA: Corwin Press: Sage.

Hinduja, Sameer, and Justin Patchin. 2014. Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying. 2nd ed. Thousand Oaks, CA: Corwin.

Johnson, Matthew. 2015. “Digital Literacy and Digital Citizenship: Approaches to Girls’ Online Experiences.” In eGirls, eCitizens, edited by Jane Bailey, and Valerie Steeves, 339–360. Ottawa: University of Ottawa Press.

Karaian, Lara. 2014. “Policing ‘ sexting’: Resposibilization, Respectability and Sexual Subjectivity in Child Protection/ Crime Prevention Responses to Teenagers’ Digital Sexual Expression.” Theoretical Criminology 18 (3): 282–299.

Kelly, Katherine, and Tullio Caputo. 2011. Community: A Contemporary Analysis of Policies, Programs, and Practices. Toronto: University of Toronto Press.

Lenhart, Amanda. 2009. Teens and Sexting: How and Why Minor Teens are Sending Sexually Suggestive Nude or Nearly Nude Images Via Text Messaging. Washington, DC: Pew Internet and American Life Project.

Limber, Susan, Maury Nation, Allison Tracy, Gary Melton, and Vicky Flrex. 2004. “Implementation of the Olweus Bullying Prevention Programme in the Southeastern United States.” In Bullying in Schools: How Successful Can Interventions Be?, edited by Peter K. Smith, Debra Pepler, and Ken Rigby, 55–80. Cambridge: Cambridge University Press.

Livingstone, Sonia, and Julian Sefton-Green. 2016. The Class: Living and Learning in the Digital Age. New York: New York University Press.

Mark, Lauren, and Katherine Ratcliffe. 2011. “Cyber Worlds: New Playgrounds for Bullying.” Computers in the Schools 28 (2): 92–116.

Michael, Adorjan, Ricciardelli Rosemary, undefined. Privacy, and London. Surveillance. 2019a. Cyber-risk and Youth: Digital Citizenship. Privacy and Surveillance. London: Routledge.

Mitchell, Kimberly, David Finkelhor, Lisa Jones, and Janis Wolak. 2012. “Prevalence and Characteristics of Youth Sexting: A National Study.” Pediatrics 129 (1): 13–20.

Morgan, David. 1997. Focus Groups as Qualitative Research. Thousand Oaks, CA: Sage.

Pearce, Natasha, Donna Cross, Helen Monks, Stacey Waters, and Sarah Falconer. 2011. “Current Evidence of Best Practice in Whole-District Bullying Intervention and Its Potential to Inform Cyberbullying Interventions.” Journal of Psychologists and Counsellors in Schools 21 (1): 1–21.

Poltash, Nicole. 2013. “Snapchat and Sexting: A Snapshot of Baring Your Bare Essentials.” Richmond Journal of Law and Technology XIX (4): 1–24.
Ricciardelli, Rosemary, and Michael Adorjan 2018. “If a girl’s photo gets sent around, that’s a way bigger deal than if a guy’s photo gets sent around”: Gender, sexting, and the teenage years. *Journal of Gender Studies* [available ‘online first’].

Ringrose, Jessica, Laura Harvey, Rosalind Gill, and Sonia Livingstone. 2013. “Teen Girls, Sexual Double Standards and ‘Sexting’: Gendered Value in Digital Image Exchange.” *Feminist Theory* 14 (3): 305–323.

Roher, Eric. 2012. “Dealing with Off-School Conduct: Cyberbullying, Drug Dealing and Other Activities Off School Property.” *Education and Law Journal of Adolescence* 21 (2): 91–109.

Rose, Nikolas. 1996a. “Governing ‘Advanced’ Liberal Democracies.” In *Foucault and Political Reason: Liberalism, Neo-Liberalism and Rationalities of Government*, edited by A. Barry, T. Osborne, and N. Rose, 37–64. London: UCL Press.

Rose, Nikolas. 1996b. “The Death of the Social? Re-figuring the Territory of Government.” *Economy and Society* 25 (3): 327–356.

Shariff, Shaheen, and Rachel Gouin. 2006. “Cyber-Dilemmas: Gendered Hierarchies, New Technologies and Cyber-Safety in Schools.” *Atlantis* 31 (1): 27–37.

Sparks, Richard, Evi Girling, and Ian Loader. 2001. “Fear and Everyday Urban Lives.” *Urban Studies* 38 (5–6): 885–898.

Steeves, Valerie, Trevor Milford, and Ashley Butts. 2010. *Summary of Research on Youth Online Privacy*. March. Ottawa: Office of the Privacy Commissioner of Canada.

Stewart, David, and Eric Fritsch. 2011. “School and Law Enforcement Efforts to Combat Cyberbullying.” *Preventing School Failure: Alternative Education for Children and Youth* 55 (2): 79–87.

Stewart, David, Prem Shamdasani, and Dennis Rook. 2007. *Focus Groups, Theory and Practice*. London: Sage.

Strauss, Anselm, and Juliet Corbin. 1990. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Newbury Park: Sage.

Tangen, Donna, and Marilyn Campbell. 2010. “Cyberbullying Prevention: One Primary School’s Approach.” *Journal of Psychologists and Counsellors in Schools* 20 (2): 225–234.

Tokunaga, Robert. 2010. “Following You Home from School: A Critical Review and Synthesis of Research on Cyberbullying Victimization.” *Computers in Human Behavior* 26 (3): 277–287.

Twinn, Sheila. 1998. “An Analysis of the Effectiveness of Focus Groups as a Method of Qualitative Data Collection with Chinese Populations in Nursing Research.” *Journal of Advanced Nursing* 28 (3): 654–661.

Vandebosch, Heidi, and Katrien Van Cleemput. 2008. “Defining Cyberbullying: A Qualitative Research into the Perceptions of Youngsters.” *Cyberpsychology and Behavior* 11 (4): 499–503.

Van Ouytsel, Joris, Michel Walrave, and Ellen Van Gool. 2014. “Sexting: Between Thrill and Fear—How Schools Can Respond.” *The Clearing House: A Journal of Educational Strategies, Issues and Ideas* 87 (5): 204–212.

Walton, Gerald. 2005. “The Notion of Bullying Through the Lens of Foucault and Critical Theory.” *The Journal of Educational Thought* 39 (1): 55–73.