STANDARDS RESEARCH

Children's Safety and Privacy in the Digital Age

May 2020

Authors

Noah Zon, Springboard Policy

Adrienne Lipsey, Springboard Policy

Project Advisory Panel

Wendy Craig, Scientific Director, PREVNet

Samantha Fauteux, Program Manager, Prevention & Promotion - Suicide Prevention, The Mental Health Commission of Canada

Kathryn Ann Hill, Executive Director, MediaSmarts

Fardouz Hosseiny, Vice-President, Research and Knowledge Management, Royal Ottawa Mental Health Centre

Matthew Johnson, Director of Education, MediaSmarts

Gareth Jones, President, Canada Safety Council

Nimmi Kanji, Director Telus Wise, TELUS

Greg Kyllo, National Director of Program Innovation, Canadian Mental Health Association (CMHA)

Carol Todd, Amanda Todd Legacy Society

Cara Yarzab, Product Lead, Prodigy Games

Laurie Amiruddin, CSA Group

Nicki Islic, CSA Group (Project Manager)

Hélène Vaillancourt, CSA Group

Table of Contents

Executive Summary

For children growing up in Canada today, the divide between their online world and their offline one is narrower than it has ever been. Growing up means growing up online.

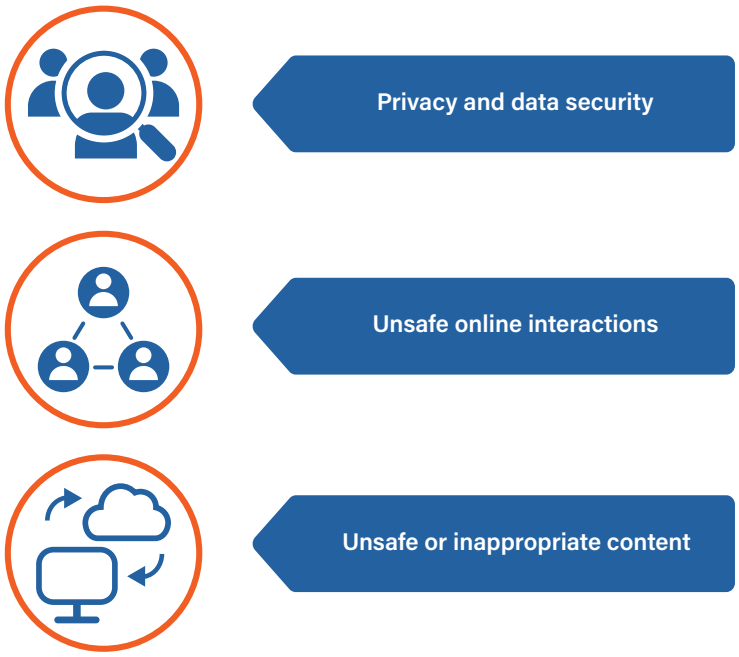
But while parents and children can rely on safety standards and regulations to ensure safe experiences for children in everything from car seats and hockey helmets to TV shows, policies and standards for online safety have not been developed to match the central role that digital tools play in learning, socializing, and expressing themselves for children and youth.

Most online services are not designed with the needs of children in mind. The entry to most space on the Internet is "guarded" by a checkbox for users to claim that they are over 13 years old. In practice, much younger children are also subject to the same data collection and exposed to the same experiences, which create real safety and privacy risks. In short, to the designers of most online services, children hardly exist.

As policymakers, standards development organizations, and industry develop new solutions and policies to address growing concerns about the digital age, such as privacy, competition, and cybersecurity, it is important that responses from industry, public policy, and standards not fall prey to the same blind spots.

To identify potential responses to promote children's safety and privacy in the digital age, this study focuses on three main areas of risk to young people's online well-being, as illustrated in Figure 1.

Figure 1: *Three Main Risks to Young People's Online Well-Being*



These risks are intertwined, as are the solutions. Through comparative international research and consultation with industry and experts, this study identifies a series of potential responses that could improve online safety and privacy for children. Some responses, like criminal law reform, are focused on specific online challenges. Others, like age-appropriate design guidelines, look more generally at ways to build a safer online world. Some of these responses call on companies to take the lead, others call on industry-wide standards, and still others call on public policy and legislation. In nearly all cases, cross-sector collaboration that engages experts and children themselves are needed to design and implement responses.

These solutions will not eliminate the online risks for children. But just as speedbumps and crosswalks can make it safer for children to navigate their neighbourhoods on foot, so too better design, standards, and policies can improve the safety of the online world; better education and resources can prepare children and parents to assess risks; and stronger institutions can address and prevent harm when it is identified. A summary of recommendations is presented in Table 1.

Table 1: *Summary of Recommendations*

Summary of Recommendations		
Privacy and data security	**Unsafe online interactions**	**Unsafe or inappropriate content**
Implement privacy by design principles	Use product design to limit risk	Develop standards for how platforms approach content moderation
Simplify Terms of Service	Standardize technical approaches to fighting child sexual abuse material (CSAM)	
Standards for security	Criminal law reform	
	Multisector partnerships	
	Education for safe online experiences	
Cross-Cutting Responses		
Investments in digital literacy curriculum	Fill research gaps	Adopt an age-appropriate design code
Age-appropriate "brackets"'	Involve children in creating solutions	Accountability mechanisms
	Create a new Office for Online Safety	

"There is no point of reference for this type of connected childhood, and no data are available about its long-term implications."

Introduction

In the last 20 years, the spread of digital technologies has transformed our world. As these technologies change the way we work, connect, and do business, they also bring new challenges to which our existing governance models, standards, and policies are ill-equipped to respond [1].

The most dramatic transformation of the digital age may be what constant connectivity means for childhood. Many parents of young children today did not have the Internet when they were their children's age — and if they did, it would likely have been dial-up connection on a shared family computer. Today, children are typically exposed to the Internet from birth: surrounded by smartphones, connected by baby monitors, tablets, computers, Internet toys, and smart homes. Nearly unlimited storage now means that the huge amounts of data being collected are stored indefinitely, often in multiple places [2].

There is no point of reference for this type of connected childhood, and no data are available about its long-term implications. Measuring the impact of something beginning in childhood over a lifetime is difficult. For example, we are only now beginning to measure the long-term effects of the arrival of the children's television show *Sesame Street* five decades ago [2]. It is more difficult to track effects in today's rapid pace of change: a 2018 European Union (EU) study found that the Internet use of tweens looks similar to the typical use of teenagers just three to four years prior, and that most children under the age of two today have some online presence through their parents [3].

What is clear, however, is that the expansion and evolution of digital technologies has not been matched by the development of systems or institutions to ensure that those technologies are safe for children. Parents, caregivers, teachers, and young people are navigating uncharted waters.

That is beginning to change. The Canadian federal government has committed to the development of a new "Digital Charter" that will include a new set of online rights. The government has also mandated that cabinet ministers work together to combat online hate and harassment [4]. Industry leaders are adopting new practices, such as Facebook's new independent oversight board [5], and YouTube has increased restrictions on data collection and targeted ads in child-directed content [6], [7]. Both non-profits and private companies are developing new approaches in technology and education that promote safer experiences for children online. And internationally, the United Nations (UN) is exploring ways to protect digital rights in the context of the UN Convention on the Rights of the Child [8].

This is challenging work that is being undertaken in a complex and fast-moving context. Technology can change significantly in the time it takes legislators to craft new laws. The Internet transcends borders and jurisdictions: regulation demands international cooperation with respect for different cultural and legal contexts.

This report considers options that can be used to lay a safe foundation for connected childhoods by considering potential responses and risks with a focus on standards, policies, and legislation. Three main areas have been taken into consideration:

- Privacy and data security;
- Unsafe online interactions; and
- Unsafe or inappropriate content.

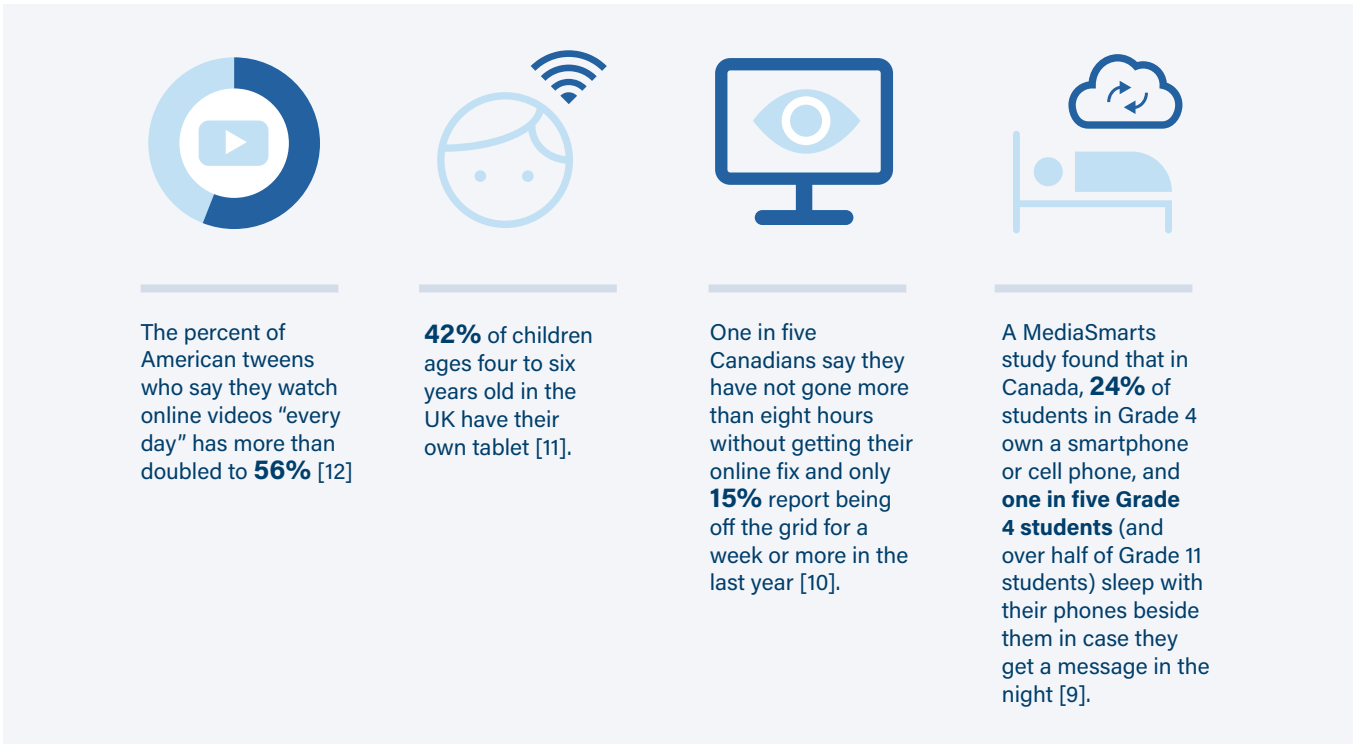
These risks are intertwined. For example, a breach in a teen's private data might be abused in the course of online harassment. Potential responses also overlap with different areas of children's online safety. This report outlines responses to each area of risk and outlines cross-cutting responses that apply to all.

About this study

This report is focused on children's online safety and privacy in Canada, and the potential role of standards in building safety that draw on international examples and best practices. It covers both children's online experiences from birth to age 18 and a full spectrum of children's online interactions from social media to Internet of Things devices.

The study draws on a review of academic and grey literature, environmental scans of industry standards development and government approaches, and eight research interviews conducted in the in fall of 2019 with experts in the field. These interviews were conducted on a background basis to allow individuals to speak freely and openly. The study also benefited from the advice of an advisory panel made up of civil society, industry, and academic experts.

Figure 2: *Connected Childhoods*



"In the online world, however, children's safety and privacy rests almost entirely in their own hands and those of their parents."

1 The challenge: Uncharted childhood

Children of all ages now rely on the Internet for school, for social connection, and for learning and playing. While this opens new opportunities, the scale of connectedness poses risks. In most other parts of their lives, children and caregivers can rely on a variety of standards and policies that ensure products and activities are safe and appropriate for children.

Take, for example, a trip to go ice skating at the community rink. There are policies on helmets and consumer-facing standards to help parents know which ones pass the test [13]. The post-skate hot chocolate is kept safe by food safety regulations and, for the ride home, there are safety standards for car seats for different ages and sizes of children.

In the online world, however, children's safety and privacy rests almost entirely in their own hands and those of their parents.

This approach may have been viable in the earlier days of the Internet, when it played a smaller role in people's lives. But today, by the time a child turns 18, they will be the subject of an estimated 70,000 social media posts about them, on average [14]. At this scale, it is impractical to personally manage privacy and data rights on a case-by-case basis.

Digital tools can also harm children's health and well-being more directly. Cyberbullying, grooming, and radicalization have led to children being exploited and harmed. Standards and regulations to create spaces and experiences that are safe for children are as important online as they are offline.

The graph in Figure 3 shows the share of users reporting adverse effects based on the age of the Internet user [15].

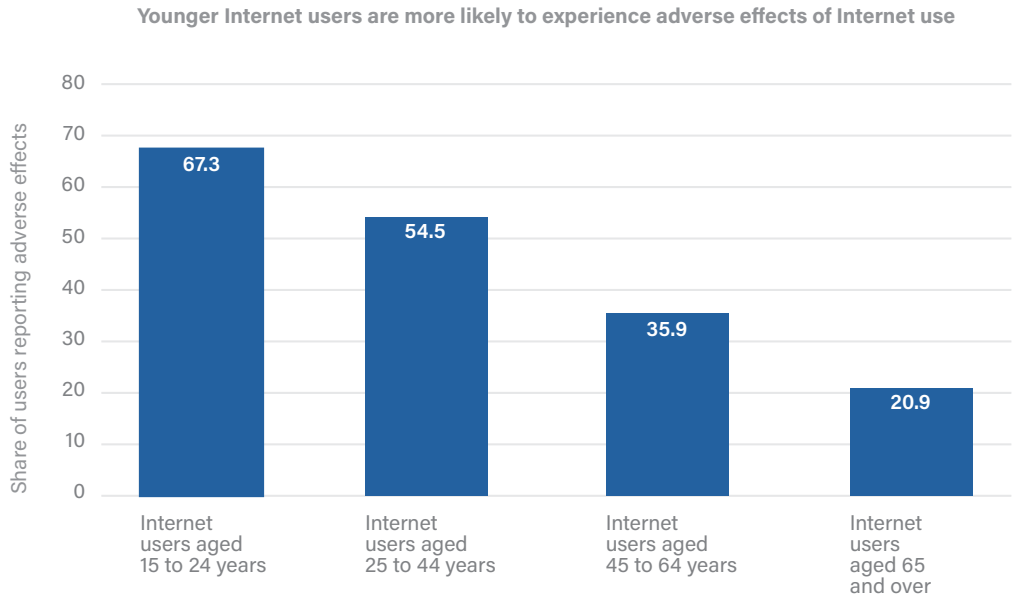
1.1. The Canadian policy and standards landscape

The wave of Internet regulation in the late 1990s and early 2000s did not envision the implications of an "always on, always connected" lifestyle, nor did it anticipate the implications of digital technologies for childhood.

Developed as part of that wave, the main consumer privacy legislation in Canada is the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). The legislation is based on the ten principles of CAN/CSA-Q830-96, *Model Code for the Protection of Personal Information* developed by the CSA Group. These principles underscore the importance of consumer consent in data collection, limitations on how data can be used, and accountability for how data are managed. The independent Office of the Privacy Commissioner of Canada (OPC) provides interpretation and guidance on the application of PIPEDA and the *Privacy Act* (which covers citizen privacy in government interactions).

PIPEDA is silent on the privacy rights of children, and the OPC has taken some steps to fill that void, saying that in general, parents must consent to the collection of data from children under 13 [16] and cautioning against the use of behavioural tracking on websites aimed at children [17].

Figure 3: *Adverse Effects on Younger Internet Users*



Source: *Statistics Canada, "Adverse Effects of Using the Internet and Social Networking Websites or Apps by Gender and Age Group" [15]. Adverse effects include, for example, anxiety, depression, trouble concentrating on other tasks, relationship issues.*

Beyond privacy, Canada has developed other policies and legislation aimed at children's online safety. The Government of Canada's 2004 *National Strategy for the Protection of Children from Sexual Exploitation on the Internet* relies heavily on partnerships between the Royal Canadian Mounted Police (RCMP) and non-profits like the Canadian Centre for Child Protection. In 2011, Bill C-22 passed and made Internet providers responsible for reporting and notifying officers "if there are reasonable grounds to believe their Internet service was or has been used to commit a child pornography offence" [18].

In the context of harmful content, policies for age-restricted products and services (e.g., tobacco, alcohol) set restrictions against marketing to children, including online.

The federal government recently committed to creating the new role of Data Commissioner, and this could enhance children's safety online. This commissioner would have the power to protect rights, including the right to data portability; to remove personal data from a platform; to monitor how data are used and to withdraw consent for sharing or selling the data; and the ability to be free from online discrimination, including bias and harassment.

1.2. The global landscape

1.2.1 United States

The relevant legislation in the United States is the *Children's Online Privacy Protection Act* (COPPA), enforced by the Federal Trade Commission. COPPA places firm restrictions on data collection about children under the age of 13. Like PIPEDA, COPPA is two decades old and adaptation to the digital age has mostly taken the form of interpretation by the regulator.

As digitization has accelerated, adequately enforcing COPPA has become challenging. A 2018 study that audited the COPPA compliance of nearly 6,000 children's apps found that the majority were not compliant. Of greater concern, one in five were collecting personally identifiable information [19].

The State of California has also introduced its own privacy legislation, the *California Consumer Privacy Act,* which was passed in 2018 with enforcement beginning in 2020 [20]. The act includes the requirement of both parental consent for children under the age of 13 and new "opt-in" measures for children aged 13 to 16 [20].

1.2.2 Europe

Experts consulted for this project emphasized that Europe has been at the forefront of advancing responses to children's online safety and privacy. The main vehicle for this work is the EU-wide *General Data Protection Regulation* (GDPR). In addition to more stringent privacy protections for all users, GDPR includes a number of measures to protect children's data privacy in the short term (limiting data collection in child-directed services) and in the long term (implementing the right to be forgotten). Because global services have good reason to be GDPR-compliant, the influence of GDPR extends beyond Europe.

Individual European states retain a great deal of latitude in regulating children's online safety more broadly. The United Kingdom (UK) has been particularly active, with government consultations on the publication of its Online Harms White Paper [21], work by civil society to develop proposals for children's digital rights [22], and a harm reduction approach to social media regulation [23]. The UK's Information Commissioner's Office has also developed an innovative Age Appropriate Design Code of Practice to inform standards of design for services likely to be accessed by children [24].

1.2.3 Global institutions

Global institutions have been active on children's online safety and privacy. In 2019, the UN Committee on the Rights of the Child published a position paper on protecting children's digital rights and invited comment from member states [25]. Other global bodies are taking the lead as well: the United Nations Children's Fund (UNICEF) developed an industry toolkit on children's online privacy and freedom of expression [26]; the Broadband Commission for Sustainable Development led a multi-year project on children's online safety [27]; and the International Telecommunication Union published guidelines for children's online protection [28]. In 2012, the Organisation for Economic Co-operation and Development (OECD) adopted a recommendation based on responses to online risks to children, and that recommendation is now being updated [29].

1.2.4 International standards

Neither the International Organization for Standardization (ISO) nor the International Electrotechnical Commission (IEC), which is responsible for developing international electrical and electronic standards, has yet developed standards on children's online safety. They have both developed guidelines for child safety in standards more generally to ensure that all standards are developed with children in mind. This guidance includes the importance of phrasing product instructions, especially safety instructions, in ways that are understandable to children [30].

The IEEE Standards Association is an organization within the Institute of Electrical and Electronics Engineers (IEEE). The association is currently developing P2089, a Standard for Age Appropriate Digital Services Framework, based on the principles developed by 5Rights, a children's digital rights charity. The work the IEEE Standards Association is completing may build on IEEE's previous work through its Global Initiative on Ethics of Autonomous and Intelligent Systems, which has made recommendations on children's data issues [31].

2 Risks and responses

This report focuses on three main risks that must be addressed if children are to thrive with safety and privacy online: privacy and data security, unsafe online interactions, and unsafe or inappropriate content.

2.1 Privacy and data security

Data privacy and security are some of the most pressing concerns of the digital age. But this is not the first time that advances in technology have compelled us to reshape our collective understanding of privacy. The arrival of the camera as a new technology over a hundred years ago led to the first efforts to define the legal right

to privacy [32]. In the past few years we have seen a new policy agenda responding to increasingly ubiquitous devices collecting sensitive data. The growth of artificial intelligence (AI) has increased concern about this risk, given the volume of data that machine learning requires and AI's capability to identify people from that data.

Privacy for children in the digital age merits special attention and distinct approaches. While privacy is important for people of all ages, for children, privacy matters as an essential part of their development [33]. This can include age-appropriate privacy from parents, meaning it is important not to over-rely on parental guardian consent as a means of protecting privacy.[1]

Historically, it has been a social norm that children's actions and experiences should not follow them throughout their lives (consider how juvenile records are expunged in the justice system) [34]. However, in the digital age, considerable detail about the experiences of youth may follow children into adulthood, with unknown implications.

2.1.2 Children do not have meaningful control over their data, and it may follow them indefinitely

Today, a rich record of photos and videos, activities, and even biometric and location data may begin for children at birth and continue through childhood as parents capture and share their information – a trend called "sharenting" [35]. Parents and grandparents often share a large volume of private information about children with good intentions but little understanding of the implications for the child's digital rights [36]. Pre-schools, camps, sports teams, and clubs often have an online presence with photos, names, and other details [37]. This pre-empts the ability of young people to make their own decisions about their privacy as this data will follow them into adulthood. This data record may have implications not only on their personal identity but also on how they are treated by public and private institutions.

We also need to consider the long tail of content created or shared by children themselves. The digital record and mass distribution made possible by the online world have different implications than a yearbook, photo album, or diary from the pre-digital age. While young people have rights to free expression, an important part of that expression in the context of adolescence is the ability to move into adulthood and define one's identity without the weight of embarrassment or indiscretion from their youth. While education about risks can be one aspect of this reality, it should also be considered carefully in policy and the design of products and services for youth.

New public policy and legal frameworks that are in place in the EU and under development in Canada look to protect emerging rights, such as the right to remove/erase personal data, often referred to as "the right to be forgotten" [4], [38]. Canada's Privacy Commissioner has argued that some rights to de-indexing (removal from search engine results without removing the original content) and to source takedown (removing personal content after consent is withdrawn) are already protected by PIPEDA, and the commissioner has filed a reference case with the Federal Court of Canada [39].

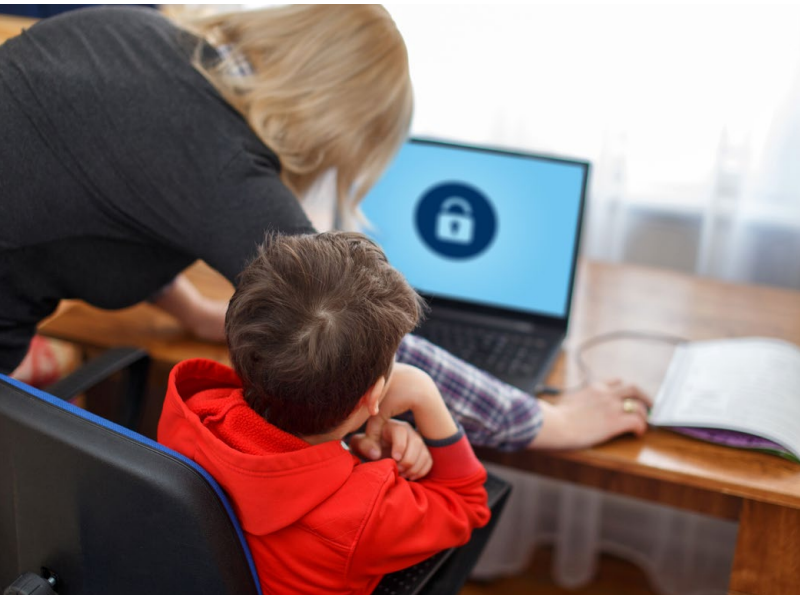
2.1.3 Informed privacy consent is a fiction

While some have called for an increased duty of care from platforms, our current systems expect parents and youth to navigate these issues and make informed choices about consent. This is unrealistic. Typical Terms of Service (ToS) agreements are long, legalistic, and offer extremely favourable terms to the platform for data collection and use [1]. Research has shown that young people are ill-prepared to make informed decisions about commercial data privacy [33].

Even where parents or young people have greater capacity to understand the implications of these agreements, opting out may not be possible. The increased use of cameras and sensors in public spaces combined with AI-powered facial recognition also places real limits on the efficacy of informed consent [40]. There is also an important social dimension to these decisions – for many children and youth, withdrawing from platforms like Instagram would be equivalent to opting out of participation in their community.[2]

[1] Research interview, 2019.

[2] Research interview, 2019.



"Given the context of children and of the design of the Internet, including dark designs and nudging, you need to ask whether consent is always the appropriate way to think about this."

—Research Interview

Schools – from elementary schools through to colleges and universities – are implementing digital tools (including cameras and smart speakers) that collect enormous amounts of data under the pretense of safety [34], [40] or improved services [42]. While the United States has a dedicated Family Education Rights and Privacy Act that limits data collection and use in schools, the act allows for widespread data collection. Proposed American legislation would even require surveillance tech in schools (as a part of preventing school shootings) [43]. Canada has no consistent approach to data privacy in schools, with parents often asked to give blanket consent to the use of services without being given information on how the data collected are being used.

2.1.4 Children's data are at risk from lax cybersecurity and data management practices

Beyond regular, legal data collection, young people's data can be inappropriately exposed when insufficient measures are in place to keep the data safe.

Cybersecurity risks increase with the number of devices we use. For example, the growing market for IoT devices has been plagued by security risks [44]. Many consumer-facing devices come with lax security practices, especially from manufacturers that are new to Internet-connected devices [44]. For example, Toymaker VTech reached a settlement with the US Federal Trade Commission in 2018, in the face of an enforcement action for failing to protect its smart toys from hackers [45].

Risks also increase with the increasing number of entities that hold a large amount of data. If data are being stored, there is a risk of disclosure. An investigation from The New York Times' Privacy Project found constant user location tracking from a school district's app among a leaked dataset [46]. External leaks are not the only risk to holding data. The New York City Police Department was also found to have kept thousands of juvenile fingerprints illegally, interfering with young people's rights to procedural fairness in the justice system [47].

2.1.5 Potential responses

Implement privacy by design principles, such as data minimization

The principles of privacy by design, initially developed in Canada by the Ontario Information and Privacy Commissioner [48], call for proactive preventative efforts to protect user privacy that are to be built into the design and default setting of services. Reducing the amount of data collected in the first place is the surest way to reduce risk of a privacy breach.

A standard for privacy by design is currently under development at the ISO to guide general best practices for consumer products [49]. Canadian guidance and regulatory approaches can ensure that their design reinforces Canadian privacy principles; the House of Commons Standing Committee on Access to Information, Privacy, and Ethics recommended that privacy by design be made a central principle of Canada's privacy legislation [50]. Some companies

are also updating their children's privacy practices to limit the data collected – for example, Mattel is taking steps to prevent or discourage children from disclosing personal information [51].

To minimize location data sharing associated with potential stalking or other safety risks, designers can limit the geolocation for devices and services marketed to children. The proposed Age Appropriate Design Code of Practice proposed by the UK's Information Commissioner recommends that devices turn off location tracking and sharing by default and that the device make it clear to children when their location is being tracked [24].

Simplify Terms of Service (ToS) to offer meaningful understanding and real choice

Even for sophisticated users, ToS agreements for most digital services are opaque. As there is no meaningful opportunity to negotiate terms [1], children face a poisoned choice between waving their digital rights and being left out of economic opportunities and social connections.

Parents and teens alike typically have a limited understanding of how they are allowing businesses to collect their data and how those businesses may use it.[3] An empirical study by legal researchers found that out of 500 ToS agreements they examined, 498 failed to meet consumer readability standards [43].

Policies and standards can play a role here. The UK Age Appropriate Design Code of Practice calls for "specific, 'bite-size' explanations" at the time that personal data are activated, with information written in child-friendly, age-appropriate terms [24]. Providing more meaningful choices can include changing default terms to opt-in rather than opt-out [50]. The 5Rights Foundation is also working with IEEE to develop a framework for ensuring meaningful age-appropriate terms and conditions for children [54].

Children in Grown-Up Spaces: Age-Gating the Internet

Creating a safe and appropriate online experience for children depends on online services being able to distinguish children from adults. The majority of platforms and services address this challenge by asking users to confirm that they are over the age of 13 – a practice known as "age-gating."[4]

But given the anonymity provided by online services – and the ability of motivated young people to effectively clear technical hurdles – the fence keeping children from the adult Internet and its attendant risks is flimsy. Stronger barriers can create a challenging tension where more information about children is needed to corroborate their age to ensure they receive enhanced privacy protections.

In most cases, services do not have any real barriers to children using their services. Instagram recently shifted from a checkbox asking users to confirm that they are 13 to requiring a birthdate – but Instagram will not be verifying the information provided [56]. There are some emergent technical solutions – for example, Yoti, a new service in the UK, can independently verify age both offline and online without sharing personal data with the businesses [57]. While these services have greater incentive to maintain stronger protections, the use of intermediaries depends on strong trust in these firms handling sensitive data. The difficulty in implementing such a system on a widespread basis led the UK government to back down from a planned national age verification system for access to pornography [58].

[3] Research interview, 2019; see also [52].

[4] Research interview, 2019.

"The fence keeping children from the adult Internet and its attendant risks is flimsy"

Standards for security

Parents and young people are also poorly equipped to navigate cybersecurity practices, especially for the growing number of IoT devices in their homes and lives. There have been calls for national and international technical standards for IoT security, highlighting practices such as unique passwords by default and ongoing security updates [44]. New legislation has been introduced in the UK that includes minimum security standards and transparency for IoT devices [55]. Another option is developing consumer-friendly labels about the security of different devices.

2.2 Unsafe online interactions

Unsafe interactions with adults or other youth online can endanger children's psychological or physical safety – what is often referred to as "contact risk"[59]. These harmful interactions may take place exclusively online or may be part of (or lead to) interactions that take place in person.

One expert in children's online behaviour interviewed for this project emphasized that young people are generally not interested in connecting with people online whom they do not already know in real life.[5] However, a minority of young people do engage in riskier online behaviours – just as they do offline.[6] A 2012 EU Kids Online survey of children between the ages of nine and 16 found that 30% had had contact online with someone they had not met face to face, and 9% had gone to a face-to-face meeting with someone they first met online [60].

Online interaction safety risks can take a number of forms, including risks of sexual exploitation; harassment, cyberbullying, and hate speech; and radicalization and extremist recruiting. Given the significant harm associated with these risks, this area of children's online safety has already seen a great deal of cooperation between industry, civil society, and law enforcement. The first Canadian federal strategy on online child sexual exploitation was launched in 2004 and has been continued and updated by successive governments, most recently with the 2019 commitments to fund prevention activities and build capacity of local law enforcement [61].

2.2.1 Risks of grooming and sexual exploitation

The most prevalent risk of online sexual exploitation for children is the creation and sharing of child sexual abuse imagery. Child sexual abuse imagery represents 95% of the reports submitted by the public to Cybertip.ca, the national tipline [62]. In a three-year period, from 2016 to

[5] Research interview, 2019.
[6] Research interview, 2019.

"In order to navigate the online world, children need to be prepared with the skills to identify and respond to risks that they may encounter."

2019, the Canadian Centre for Child Protection reported the detection of 13 million suspected images of child sexual abuse [63]. A US study of teens found that one in 20 had been the victim of "sextortion," which happens when someone threatens to share intimate images that were either initially shared voluntarily or hacked unless something is given in return (often more images) [64].

Online interactions are a source of risk for grooming or luring for sexual exploitation or human trafficking. Predators can use online communication to build trust, isolate, and entrap the child for abuse [65]. The anonymity afforded by online interactions allows offenders to use rapport-building tactics not available offline, such as desensitization to sexual topics [65]. The risks of these online interactions do not only come from other adults – a large share of child sexual abuse material (CSAM) is shared by other minors.

2.2.2 Consumer risks and scams

While in many ways young people are more adept with digital tools than their parents, children face an increased risk of online fraud and scams as they may be less well-positioned to identify fraud risks. A 2018 US study estimated that over one million children had been the subject of identity theft in the past year, representing USD $2.6 billion in losses [66]. A data record from an early age with long-forgotten accounts and poor data management practices put children at increased risk of identity theft.

Children who are vulnerable face increased risk — the Identity Theft Resource Center found that youth in care are more likely to have credit cards opened in their name without their knowledge or consent, and are less likely to have support and resources to protect their identity [67]. Barclays, a global financial services company, has warned that parents may put their children at increased risk of future fraud by sharing personal details online that make them more vulnerable to identity theft [68].

2.2.3 Cyberbullying

While definitions and measurement vary, the Pew Research Center found that six in 10 US teens reported experiencing cyberbullying [69]. Compared to offline bullying, cyberbullying may be characterized by increased intensity driven by anonymity and physical distance, a risk of "viral" sharing to increase exposure, and reduced visibility to parents and teachers [70].

Cyberbullying can happen in a variety of forms and contexts, including bullying through chat on social media or video games, posting images or videos, and negative comments on photos or other content shared online by children [71].

Cyberbullies can follow children home and reach them at all hours. The impact of this "all-encompassing" experience can be profound. Victims of cyberbullying are twice as likely to self-harm as their peers [71]. As with other forms of bullying, there are intersectional

factors that might make some children more likely to experience cyberbullying, with high rates among LGBTQ+ youth and racialized youth.

Platforms have faced pressure to strengthen their anti-harassment policies to prevent cyberbullying. For example, in December 2019, YouTube updated its harassment and hate speech policies to address a wider range of behaviours, having already suspended the ability to comment on most videos featuring minors [72], [73]. Unlike YouTube, smaller platforms typically disclose very little about their practices and face little accountability [74].

When it comes to public policy, most responsibility related to cyberbullying in Canada rests within provincial jurisdiction: in particular, schools and mental health resources. When harassment crosses the line to criminality, federal criminal law is implicated. Some provinces have specifically amended legislation to define cyberbullying. While some advocates have recommended Criminal Code updates to address cyberbullying, a working group of federal, provincial, and territorial experts concluded that cyberbullying is effectively covered by existing parts of the Code [77].

2.2.4 Radicalization and recruitment to extremism

Radical extremist groups use online forums to recruit when they cannot make physical contact with their target. This allows them to recruit from a wider pool, which is a process that a former recruiter described as moving from "retail to wholesale levels" [75]. While terrorist groups such as ISIS continue to use social media for recruitment, they are increasingly being pushed off of major platforms to alternative and "darknet" platforms (though this is less true of far-right extremism more generally) [76].

These groups often use similar grooming tactics as those used in sexual exploitation in targeting Canadian teens [77]. In the case of ISIS targeting young women, radicalization and human trafficking are intertwined [78]. As part of the Government of Canada's 2018 *National Strategy on Countering Radicalization to Violence,* Public Safety Canada placed emphasis on both countering online radicalization and engagement with youth [79].

YouTube has been criticized for its role in radicalization, in particular through its platform's recommendation engine [80]. While the degree to which its design actively encourages radical content is the subject of some debate, YouTube has acknowledged the troubling role of harmful as well as "borderline" content on the platform and has changed its algorithm and policies, claiming that more stringent policies combined with investments in machine and human moderation to enforce those policies have decreased the viewing time of these videos significantly [81], [82].

2.2.5 Increased risks from IoT

As children's online experiences increasingly include a variety of connected devices, intersections with privacy and security risk can mean new, potentially more invasive exposure to unsafe interactions. While publicized cases (like a hacked home security camera being used to shout racial slurs at children in Tennessee [83]) may be exceptional, they demonstrate the increased sensitivity associated with IoT and the need for appropriate responses. Wearable devices and augmented reality features also expose young people to more prominent and targeted advertising [84].

2.2.6 Potential responses

Responses to these risks must strike a balance between children's competing rights to be safe and their rights to privacy, free expression, and access to information.

For example, TikTok, a video-sharing social networking service, found that a disproportionate share of cyberbullying on its platform was directed at users with disabilities. However, TikTok's initial response was to secretly limit the viewership of videos depicting individuals with visible disabilities, which itself discriminated against users with disabilities by limiting their opportunities for expression [85]. Risks to freedom of expression and to privacy also arise when parents use tools intended to protect their children in order to

delete posts that the parents simply do not like, or do so without their children's knowledge.[7]

Law enforcement also has access to a wider range of tools, including those intended to protect children from exploitation and radicalization. But these must be used in compliance with privacy and civil rights. Proposed Canadian legal reforms on cyberbullying in 2014 faced broad criticisms from stakeholders over granting law enforcement with powers to access personal data [126].

Use product design to limit risk

The way many online services are designed – especially social media – can encourage harmful interactions. Apps that encourage anonymous feedback aimed at teens have unsurprisingly fostered bullying and harassment [86]. A child development expert interviewed for this project praised the decision by Instagram to no longer display the number of "likes" on each post; this change may help to reduce those attention-seeking behaviours in users of all ages that encourages risky behaviour and amplifies cyberbullying.[8]

Standardize technical approaches to fighting CSAM online

Efforts by platforms, law enforcement, and tiplines to identify and remove offending material are hampered by inconsistent approaches. The Child Dignity Alliance has called for multilateral efforts to build a single standard framework for the classification of images [87]. The Luxembourg Guidelines, an international interagency effort to harmonize approaches, provides a foundation for this effort, but greater ongoing cooperation is needed [88].

Criminal law reform

Many online offenses related to harmful online interactions with children are prosecuted under laws that were written in the pre-Internet age. The time is ripe for updating these laws.

For example, a working group of federal, provincial, and territorial officials have recommended that a new criminal offence be developed in the Criminal Code specific to non-consensual distribution of intimate images, and that some provisions related to cyberbullying be clarified. Some members of the working group felt that this change was imperative to deal with cases not captured by current child pornography clauses under the Code; for instance, where the perpetrator is also under 18 years of age [89]. The UK made sexual communication with a child a distinct criminal offense in 2017 [90]. The Canadian Centre for Child Protection has called for a more expansive definition in the *Criminal Code* related to harmful/abusive images to account for the full range of abusive images (in particular images of physical abuse) [63]. Law reform can also include expanding restorative justice initiatives, such as those led by the Boys & Girls Clubs of Canada [91].

Partnerships between civil society, law enforcement, and industry

In 2018 consultations on the *National Strategy for the Protection of Children from Sexual Exploitation,* stakeholders recommended connecting civil society and industry experts through a pan-Canadian coalition of non-governmental organizations (NGOs) and government officials to share knowledge and build solutions together [92]. They also called for standardized best practices for safe online services by industry [92].

Cooperation with industry can help spread best practices. Microsoft, for example, has developed an automated system that can help identify potential cases of grooming in online chats, with content reviewers then flagging relevant cases to law enforcement [93]. An increasing array of technical tools can also detect and eliminate CSAM [94].

International cooperation is also required, since child safety online is an international problem. When some countries allow perpetrators to operate with impunity, children across the world can be harmed. While

[7] Research interview, 2019.

[6] Research interview, 2019.

"There's a duty of care that starts right at the beginning when you're designing a platform that you're encouraging people to share content on."

—Research Interview

many harmful online interactions are local in nature, the borderless Internet depends on international cooperation among law enforcement. The Child Dignity Alliance reports that 35 countries have no laws making child sexual abuse imagery a crime, and many other countries have laws that are poorly defined and enforcement that is poorly resourced [95].

Educational activities to prepare children for safe online experiences

In order to navigate the online world, children need to be prepared with the skills to identify and respond to risks that they may encounter. An integrated approach to cyberbullying in a safe schools strategy has been a key contributor to Finland achieving rates of bullying that are among the lowest in the world.[9] The World Childhood Foundation worked with researchers at the University of Skövde to develop an interactive board game that helps children build safety responses to real-life grooming tactics (while ensuring the game itself is free from inappropriate content) [96]. The LEGO Group's online platform "LEGO Live" was highlighted by a non-profit leader interviewed for this study as an example of building on research to create a safe environment for children to learn how to communicate online and use social networking tools.[10]

Parents would also benefit from learning supports. A researcher interviewed for this project recommended using online safety programming for parents to complement curriculum for children, starting from an early age in school.[11] Approaches that focus on restricting access in response to risky behaviour, for example, may discourage children from telling their parents about a harmful or dangerous experience.

2.3 Unsafe or inappropriate content

As children explore an online world that is designed for adults, they face the risk of being exposed to harmful or age-inappropriate content that can include violent imagery, hate speech, or content that encourages self-harm [97]. In contrast to unsafe interactions, this risk does not require that there be a person on the other end of the content – it is enough for unsafe content to be accessible online. There are also potential risks associated with the role that "screen time" plays at critical times in cognitive and physical development, including evidence that some online technologies are addictive. Online content and screen time are among the top concerns Canadian parents have about Internet safety [98].

[9] Research interview, 2019.
[10] Research interview, 2019.
[11] Research interview, 2019.

"We need to see more leadership on education. In the 1980s Ontario was among the first in the world to introduce media literacy into the curriculum. Now we are falling behind."

—Research Interview

A survey of 10,000 children in the EU between the ages of nine and 16 found that pornography (named by 22% of children who mentioned risks) and violent content (named by 18%) were among the top concerns children had when interacting with the Internet [60]. Exposure to harmful content can provoke a host of mental health issues including depression, anxiety, and social isolation, aggression and violence, cognitive problems, post-traumatic stress disorder, and addictive behaviours [99].

Legal and regulatory approaches to unsafe content are limited to certain types of content, such as CSAM, or certain types of hate speech. Most tools to protect children from unsafe content rest with online service providers, parents, and young people themselves. Platforms generally address these issues through their own ToS agreements, supported by human and automated content moderation (such as the option of content filters). Changes are often iterative and develop as platforms develop and grow. For example, in early 2020, TikTok updated its community guidelines for its platform that included a ban on videos depicting underage substance use, violent or graphic content, hate speech, and harassment [100].

2.3.1 Disturbing, violent, or sexually explicit material

The most common risk of harmful online content for children is exposure to material that they find disturbing, including violence and pornography. Surveys suggest that children are most likely to encounter this content on video-sharing sites or on social media [101]. The recommendation/autoplay features of these services are a major feature in exposing children to risk, along with content that may be shared into their feeds by peers or people they follow.

On sites like YouTube, a worrying trend has emerged of easier accessibility to disturbing and inappropriate content that on the surface looks like familiar child-friendly content but in fact includes a variety of disturbing material that has been spliced in [102], [103]. This has included content that makes use of popular children's characters like Peppa Pig in videos that encourage self-harm [104]. The growing popularity of live-streaming sites like Twitch make content moderation more challenging.

To address the risk of exposure to pornographic content, the UK sought to develop a legal requirement for age verification (known as age-gating) to prevent minors from accessing pornographic material online, as part of its broader strategy to reduce the risk of online harms [21]. The plan was for this age-gating to have an in-person component. This was met with a number of technical and political hurdles and was ultimately abandoned by the government shortly before it was due to launch [58].

Apart from sexual and violent material, young people may face exposure to content that encourages, normalizes, or triggers self-harm or suicide [105]. In numerous

studies, youth mental health researchers have found a link between exposure to self-harm content online and incidents of self-harm or suicide, although the causality is unclear [21].

Online services are also the site of new forms of self-harm. This includes young people sharing embarrassing or harmful content about themselves and anonymously sending cyberbullying content to themselves from fake accounts [106]. Children who engage in other forms of self-harm are more likely to engage in digital self-harm [106].

Approaches to moderating content related to self-harm online should be careful to avoid overly blunt approaches. A systematic review of independent studies found that alongside significant potential for harm, the Internet provides important access to crisis support and services [105].

2.3.2 Discrimination and hate speech

Children of all ages may be harmed by exposure to hateful content online. In a 2014 survey of Canadian students from Grades 7 to 11, 37% reported that they were exposed to racism and sexism online at least once a day or once a week [107]. In the UK in 2017, 45% of children aged 12 to 15 reported seeing hateful content online [108].

For adolescents of colour in particular, exposure to online racism has been shown to be harmful to mental health and developmental outcomes, associated with depressive symptoms, anxiety, and other performance-related factors (e.g., academic achievement and increased problem behaviour) [109]. These impacts are likely similar for other marginalized groups, for instance LGBTQ+ youth. Hate speech also has an effect of silencing the targets of that speech, preventing those young people from exercising their digital rights [23].

2.3.3 Screen time

According to a study by Common Sense Media, between 2015 and 2019, the share of children who watched videos online doubled, and the amount of time they spent on average watching also doubled [12]. The same study found that as access increased, the screen time for children in higher-income households decreased by one hour and 45 minutes per day when compared with their lower-income counterparts, which may be explained by the fact that parents with greater resources have more options help their children make choices to limit screen time in favour of other activities.

The evidence of the effects of screen time remains mixed. Understandably, there are no longitudinal data measuring the effects of devices and services that have only emerged recently. The Canadian Paediatric Society recommends moderate use for adolescents, along with focusing on the quality of healthy online use [110]. The World Health Organization has recommended very limited screen time for children under the age of five, though these recommendations are driven more by an emphasis on keeping children active than on the effects of screen use [111]. By contrast, research from the Oxford Internet Institute suggested that moderate screen time was associated with better outcomes than very limited online engagement [112]. Children with autism spectrum disorder have increased risk factors for harmful effects of technology overuse [113].

Online services have become very effective at maximizing users' attention, and children are no exception. The analytics provided by YouTube and streaming services such as Netflix allow content creators to understand with precision where viewing drops off in a video in order to optimize viewership [114]. While this means improved quality of products that give users what they want, it also means greater success at drawing users – including young children – in to watching for longer. Device manufacturers and online services are increasingly building screen time management into their toolkits for online privacy and safety. Screen time monitoring and limits now come pre-installed on many devices, in particular those made for children.

Researchers and parents have highlighted concerns around overuse of online gaming. The World Health Organization has added "gaming disorder" to its international classification of diseases, though other researchers have questioned the evidence behind this decision [115], [116].

2.3.4 Potential responses

Develop standards for how platforms approach content moderation

Article 19, a non-profit focused on freedom of expression, has called for a "Social Media Council" – a multistakeholder accountability mechanism to address content moderation issues based on international human rights standards [117]. Global Partners Digital has also called for a set of "Online Platform Standards" to deal with how platforms should handle harmful content and that would be monitored by an independent global oversight body [118]. Canadian academics have called for a set of standards on how platforms approach content moderation, and for a standards body that would not moderate content itself but would ensure consistent standards-driven approaches to how moderation is done [119]. Appropriate care needs to be given to the design of any independent adjudicator to ensure that it is neither window-dressing nor powerful but unaccountable [119].

Content moderation standards could also address the working conditions of human content moderators. In addition to their exposure to large volumes of disturbing content in the course of their roles [120], there have also been multiple reports of work environments that are profoundly damaging to employees [121].

3 Cross-cutting responses

Many of the potential responses to the risk of online harms to children are not unique to one type of harm but instead focus on building a stronger foundation for children's online safety and privacy. In addition to the responses to specific harms identified throughout this report, this section maps potential cross-cutting responses.

3.1 Investments in digital literacy curriculum

A common theme in research on children's online safety – and one underscored by the experts we spoke to for this study – is the importance of educating children of all ages and their guardians about online safety and privacy risks and the strategies to navigate them.

Despite the important role that the Internet plays in young people's lives, digital literacy and safety does not receive the same level of priority in safety education as other risks. Child safety experts have called for digital literacy instruction to be "mainstreamed," making it a core part of the curriculum for all subjects [11].

It is also important to develop corresponding resources for parents and for educators – many of whom themselves have a limited understanding of online risks. One expert told us that parents typically learn technology in the workplace, and this learning may offer a poor basis for setting norms about technology use at home. For example, a workplace understanding of technology may lead parents to enforce more restrictive monitoring for their children, which is not effective in the long run, and may make children less likely to talk to their parents about the risks they encounter online.[12]

3.2 Fill the research gaps

Policymakers and researchers will need better investments in research to build effective strategies for children's online safety and privacy, and also to evaluate their effectiveness. We heard from experts that Canada is far behind its peer countries in our level of research into children's online safety – a conclusion that was reinforced by the literature review conducted for this project. There are fewer and smaller sources of ongoing funding for research to understand children's online safety and privacy in Canada compared to its peer countries. For example, while the communications regulatory body in the UK funds regular comprehensive research on digital literacy and safety, Canadian researchers cannot acquire the resources to do wide-ranging studies.[13]

Beyond funding, there is a problem with insufficient data about children's online habits being collected by legitimate research sources, such as Statistics Canada. Beyond a certain irony – there is not enough data

[12] Research interview, 2019.

[13] Research interview, 2019.

"There's a problem if you take a broad-brush approach to children under the age of 18. A two-year-old's privacy needs are different than a 15-to-18-year-old's"

—Research Interview

collected about, among other things, what data are collected – this is a problem because having insufficient data hampers research into the harms that children could encounter.

3.3 Adopt an age-appropriate design code

The best prevention methods for children's online activity is to build the principles of privacy and safety into the design of products and services from the outset. Designing for the needs of younger users – setting privacy protections by default, providing clear information about data collection from connected devices – also leads (in most cases) to services that better serve consumers of all ages.

Regulators in the UK and Australia have developed codes of practice to guide industry in designing for privacy and safety. The UK's Age Appropriate Design Code of Practice sets out 15 principles with specific design direction to support companies, both in complying with GDPR and to build products that serve the best interests of children [24]. In Australia, the eSafety Commissioner developed a set of safety by design principles and is now working on a guidance framework for the industry [122]. Outside of government, the IEEE is working with 5Rights on a Standard for Age Appropriate Digital Services Framework [54].

Standards and guidance for children's online safety and privacy can provide a clear set of shared principles to help companies assess their services to ensure they are providing a safe environment for children. They can also form a basis for regulation for assessment and labelling: these help parents and young people evaluate whether a product or service meets these principles without having to examine every setting themselves.

3.4 Use age-appropriate "brackets" when developing standards and regulations for online activity

In addressing children's safety and privacy, the Internet tends to operate in binaries: asking if users are over or under 13, or over or under 18. While this broadly mimics how society understands childhood and adulthood in legal frameworks, it does not reflect more robust ways that we work to ensure age-appropriate development and safety in policy and standards.

When standards are designed to support and protect children, they usually are "fenced" or benchmarked by age or stage of development. For example, safety guidance for sports and playgrounds or content ratings for TV, movies, and video games are geared to age brackets, based on typical physical and psychosocial development milestones. While these are not perfect – no two children are the same – they provide a benchmark for parents and children to make better decisions. Few standards on the Internet reflect this level of nuance, and they would not be easily enforceable if they did.

However, there is still significant value in building tools and standards for children's online safety and privacy to reflect how children develop. For example, the UK's Age Appropriate Design Code of Practice sets out five "buckets" from ages zero to 17 to reflect different developmental stages, and outlines skills, capacities, needs, and behaviours for each [24].

3.5 Involve children in creating solutions

Involving young people in design and policymaking both helps to ground efforts in children's digital rights and ensures that solutions reflect children's realities. As one researcher told us, "The best way to learn about the way young people use technology is from kids themselves."[14] It is very rare for children to be invited to participate in policies, standards, or practices at national or international levels [123].

Some governments have introduced consultations and co-development initiatives to get input from youth. The UK Cabinet Office's Policy Lab has built a youth steering group made up of 14-to-24-year-olds to inform the government's approach and test its digital policy solutions [124]. Similar youth consultative bodies exist in Canada, unrelated to digital policy. The federal government could work with the existing Prime Minister's Youth Council to design youth-focused consultations to get input into the new Digital Charter and related policy changes.

3.6 Accountability mechanisms

Strong policies and standards are only effective where enforcement mechanisms are powerful and easy to use [120]. Most enforcement of online safety – whether by a public body or by a platform that chooses to enforce its ToS agreements – depends on people bringing forward complaints. However, complaints processes are often difficult to understand or navigate, and may not have users' trust, especially when users do not believe the platform or regulator will act. These hurdles are particularly high for children, and doubly so for those in the midst of online harm.

Both platforms and regulators can address this issue in part by working with "super-complainants" mechanisms to empower civil society groups to bring complaints on behalf of users. The UK uses this type of partnership with civil society groups to build accountability and oversight in a variety of areas, including consumer protection.[15] Article 80 of the GDPR allows EU member states to designate non-profits to play this type of role. Platforms themselves also work with many of these groups to act as "trusted flaggers" on their platforms, providing groups with resources and access to allow them to amplify children's voices and advocate on their behalf.[16]

3.7 Create a new Office for Online Safety

In Canada today, policy and regulatory responsibility for children's online safety is divided between different parts of government and independent regulators. Each of these actors – privacy commissioners, law enforcement agencies, telecommunications regulators – are influenced and limited by their own mandates, with none empowered to look at protecting the full range of risks and response to children's online safety [125].

In 2015, the Australian government introduced new legislation that created a national eSafety Commissioner. This commissioner has both enforcement powers related to online safety and a mandate to promote research and resources for safe online experiences. Creating a similar office in Canada was a key recommendation emerging from the federal government's 2018 consultations on the *National Strategy for the Protection of Children from Sexual Exploitation on the Internet* [92]. The Broadband Commission for Sustainable Development – a joint initiative of the United Nations Educational, Scientific, and Cultural Organization (UNESCO) and the International Telecommunications Union (ITU) – has also recommended a single national authority with responsibility for children's online safety [27]. A new Office for Online Safety in Canada could be given a mandate to coordinate policy and initiatives across the different strategies and policies aimed at children's online safety and privacy and be responsible for publishing research and resources that would support safer online experiences.

[14] Research interview, 2019.
[15] Research interview, 2019.
[16] Research interview, 2019.

"There are very few options for users to raise grievances. There are a few channels with law enforcement, otherwise their only choice is to go to the media"

—Research Interview

4 Conclusions

For children growing up in the digital age, their ability to safely navigate their online experiences is as essential as their ability to safely explore their neighbourhoods. We teach children how to act safely when walking to and from school, but we also build sidewalks, crosswalks, and speedbumps, and even provide crossing guards to keep them safe. For their online life, most experiences are closer to telling them to stay safe while crossing a six-lane highway without a signal.

The risks of online harms are not typically as stark or as tangible as a truck travelling at 100 km/h. But the risks are real and can have significant – and sometimes devastating – consequences for children in the near term and long term.

In response to increased public concern and breaches of public trust, governments and large platforms are beginning to redesign policies and governance for data collection, security, and privacy. Canada's 20-year-old consumer privacy regime may need a long-overdue overhaul in order to respond to the realities of the digital age.

When consumer privacy legislation was first developed, it was largely silent on the rights and needs of children. As a result, the bulk of online services are not designed with the needs and interests of children in mind. Because we have so little research about young people's online experiences in Canada, and because young people are so rarely given a voice in these conversations, we are at risk of the new set of digital governance institutions being designed without an understanding of children's rights once again.

We can take action to improve the design of online services to protect children's safety and privacy and develop methods to make companies and institutions more accountable for children's digital rights. Some of those steps would include changes to law and regulation. Industry standards, backed by certification or regulation, can also play a role in helping parents, children, and institutions make safer choices. Investments in digital literacy can help children and parents better understand how to navigate the digital age. Importantly, companies can show leadership by implementing age-appropriate design features throughout their products.

Today we are witnessing the first generation to grow up with smartphones, tablets, and connected devices constantly present in their lives. These tools connect them to information, family, and creative opportunities. But like any tool, they can be dangerous if not used safely, especially for children. As we design the digital landscape for our evolving online world – a world that is different than that which any adult decision-makers occupied as children – we have a duty of care to ensure safety for its youngest occupants.

A summary of our recommendations are included in Table 2.

Table 2: *Recommendations for Designing a Safer Online World*

Summary of Recommendations		
Privacy and data security	**Unsafe online interactions**	**Unsafe or inappropriate content**
Implement privacy by design principles *Lead: standards development organizations (SDOs) and industry*	Use product design to limit risk *Lead: industry*	Develop standards for how platforms approach content moderation *Lead: standards development organizations (SDOs)*
Simplify Terms of Service (ToS) *Lead: standards development organizations (SDOs) and industry*	Standardize technical approaches to fighting child sexual abuse material (CSAM) *Lead: standards development organizations (SDOs) and government*	
Standards for security *Lead: standards development organizations (SDOs)*	Criminal law reform *Lead: government*	
	Multisector partnerships *Lead: multisector*	
	Education for safe online experiences *Lead: government*	
Cross-Cutting Responses		
Investments in digital literacy curriculum *Lead: government*	Fill research gaps *Lead: government*	Adopt an age-appropriate design code *Lead: government and standards development organizations (SDOs)*
Age-appropriate "brackets" *Lead: standards development organizations (SDOs)*	Involve children in creating solutions *Lead: multisector*	Accountability mechanisms *Lead: industry and government*
	Create a new office of online safety *Lead: government*	

References

[1] K. Alwani and M. C. Urban, "The digital age: Exploring the role of standards," CSA Group, Toronto, On, CAN, May 2019. Available: https://www.csagroup.org/wp-content/uploads/CSA-Group-research-Digital-Economy.pdf

[2] S. Chaudron, R. D. Gioia, and M. Camp, "Young children (0-8) and digital technology – A qualitative study across Europe," EU Science Hub – European Commission, Jan. 22, 2018. [Online]. Available: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/young-children-0-8-and-digital-technology-qualitative-study-across-europe.

[3] M. S. Kearney and P. B. Levine, "Early childhood education by television: Lessons from Sesame Street," *Am. Econ. J. Appl. Econ.,* vol. 11, no. 1, pp. 318–350, Jan. 2019, doi: 10.1257/app.20170300.

[4] Rt. Hon. Justin Trudeau, "Minister of Innovation, Science and Industry Mandate Letter," Prime Minister of Canada, Dec. 13, 2019. [Online]. Available: https://pm.gc.ca/en/mandate-letters/minister-innovation-science-and-industry-mandate-letter

[5] B. Harris, "Establishing structure and governance for an independent oversight board," Facebook Newsroom, Sep. 17, 2019. [Online]. Available: https://about.fb.com/news/2019/09/oversight-board-structure/

[6] R. Jennings, "Kids' YouTube as we know it is over. Good," *Vox,* Dec. 20, 2019. [Online]. Available: https://www.vox.com/the-goods/2019/12/20/21025139/youtube-kids-coppa-law-ftc-2020

[7] R. Tracy, "YouTube to limit data collection on children's videos," *The Wall Street Journal,* Dec. 30, 2019. [Online]. Available: https://www.wsj.com/articles/youtube-to-limit-features-on-childrens-videos-irking-creators-11577701800

[8] S. Livingstone, "Rethinking the rights of children for the Internet Age," LSE Blog, Mar. 12, 2019. [Online]. Available: https://blogs.lse.ac.uk/impactofsocialsciences/2019/03/12/rethinking-the-rights-of-children-for-the-internet-age/

[9] V. Steeves, *Young Canadians in a wired world, phase III: Trends and recommendations.* Ottawa, ON, CAN: MediaSmarts, 2014. [Online]. Available: https://mediasmarts.ca/sites/mediasmarts/files/publication-report/full/ycwwiii_trends_recommendations_fullreport.pdf

[10] Canadian Internet Registration Authority, "Canada's Internet Factbook 2019," CIRA. [Online]. Available: https://www.cira.ca/resources/corporate/factbook/canadas-internet-factbook-2019 (accessed Feb. 14, 2020).

[11] T. Burns and F. Gottschalk, "What do we know about children and technology?" OECD, 2019. [Online]. Available: https://www.oecd.org/education/ceri/Booklet-21st-century-children.pdf

[12] V. Rideout and M. Robb, "The 2019 common sense media census: Media use by tweens and teens," Common Sense Media. [Online]. Available: https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens-2019 (accessed Feb. 25, 2020).

[13] "Public & Leisure Skating," City of Toronto. [Online]. Available: https://www.toronto.ca/explore-enjoy/recreation/skating-winter-sports/public-leisure-skating/ (accessed Jan. 1, 2020).

[14] Children's Commissioner for England, "Who knows what about me?" CCE, Nov. 18, 2018. [Online]. Available: https://www.childrenscommissioner.gov.uk/publication/who-knows-what-about-me/

[15] Statistics Canada, "Adverse effects of using the Internet and social networking websites or apps by gender and age group," Table: 22-10-0114-01. [Online]. Available: https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=2210011401 (accessed Jan. 8, 2020).

[16] Office of the Privacy Commissioner of Canada, "Collecting from kids? Ten tips for services aimed at children and youth," OPCC, Dec. 14, 2015. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/business-privacy/bus_kids/02_05_d_62_tips/

[17] Office of the Privacy Commissioner of Canada, "Guidelines on privacy and online behavioural advertising," OPCC, Dec. 17, 2015. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/gl_ba_1112/

[18] Parliament of Canada, "Government Bill (House of Commons) C-22 (40-3) – Royal Assent – An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service." [Online]. Available: https://www.parl.ca/DocumentViewer/en/40-3/bill/C-22/royal-assent/page-44#5 (accessed Jan. 8, 2020).

[19] I. Reyes et al., "'Won't somebody think of the children?' Examining COPPA compliance at scale," *Proc. Priv. Enhancing Technol.,* vol. 2018, no. 3, pp. 63–83, Jun. 2018, doi: 10.1515/popets-2018-0021.

[20] State of California Department of Justice, "California consumer privacy act (CCPA)," Office of the Attorney General, Oct. 16, 2018. [Online]. Available: https://oag.ca.gov/privacy/ccpa

[21] UK Department for Digital Media, Culture and Sport, *Online Harms White Paper,* Apr. 2019. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

[22] 5Rights Foundation, "Children and young people's rights." [Online]. Available: https://5rightsfoundation.com/our-work/childrens-rights/ (accessed Jan. 15, 2020).

[23] W. Perrin and L. Woods, "Reducing harm in social media through a duty of care," Carnegie UK Trust, May 8, 2018. [Online]. Available: https://www.carnegieuktrust.org.uk/blog/reducing-harm-social-media-duty-care/

[24] Information Commissioners Office, "Age appropriate design: A code of practice for online services," ICO, Feb. 5, 2020. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/

[25] UN Committee on the Rights of the Child, "General comment on children's rights in relation to the digital environment," Office of the High Commissioner of Human Rights, Mar. 2019. [Online]. Available: https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx (accessed Feb. 25, 2020).

[26] UNICEF, *Industry toolkit: Children's online privacy and freedom of expression,* UNICEF, New York, NY, USA, May 2018. [Online]. Available: https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf

[27] Broadband Commission for Sustainable Development, *Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online,* BCSD Working Group on Child Online Safety, Paris, France, Oct. 2019. [Online]. Available: https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf

[28] International Telecommunications Union, *Guidelines for Children on Online Protection,* ITU, Switzerland, Geneva, 2nd ed., 2016. [Online]. Available: https://www.itu.int/en/cop/Documents/S-GEN-COP.CHILD-2016-PDF-E[1].pdf

[29] OECD, "Protecting children online," OECD. [Online]. Available: https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdfhttps://www.oecd.org/sti/ieconomy/protecting-children-online.htm (accessed Jan. 17, 2020).

[30] *Safety Aspects — Guidelines for Child Safety in Standards and Other Specifications,* ISO/IEC Guide 50:2014, International Standards Organization and International Electrotechnical Commission, Geneva. Switzerland, Dec. 2014. Available: https://www.iso.org/standard/63937.html

[31] IEEE, "Personal Data and Individual Agency," IEEE. [Online]. Available: https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead1e_personal_data.pdf (accessed Feb. 25, 2020).

[32] S. D. Warren and L. D. Brandeis, "The right to privacy," *Harv. Law Rev.,* vol. 4, no. 5, pp. 193–220, 1890, doi: 10.2307/1321160.

[33] M. Stoilova, S. Livingstone, and R. Nandagiri, "Children's data and privacy online: Growing up in a digital age, an evidence review, Research findings," London School of Economics and Political Science, London, UK, 2019. [Online]. Available: http://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf

[34] K. Eichhorn, "Why an internet that never forgets is especially bad for young people," *MIT Technology Review,* Dec. 27, 2019. [Online]. Available: https://www.technologyreview.com/s/614941/internet-that-never-forgets-bad-for-young-people-online-permanence/

[35] L. Plunkett, Sharenthood: *Why We Should Think Before We Talk About Our Kids Online.* Cambridge, MA, USA: MIT Press, 2019.

[36] K. Notopolous, "Baby Boomers Can't Stop Sharing Photos Of Their Grandkids. Millennial Parents Aren't Happy." BuzzFeed News, Jul. 5, 2019. [Online]. Available: https://www.buzzfeednews.com/article/katienotopoulos/the-biggest-risk-to-your-childs-online-privacy-grandma

[37] T. Lorenz, "When kids realize their whole life is already online," *The Atlantic,* Feb. 20, 2019. [Online]. Available: https://www.theatlantic.com/technology/archive/2019/02/when-kids-realize-their-whole-life-already-online/582916/

.

[38] "What are my rights?" European Commission. [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_en (accessed Jan. 4, 2020).

[39] Office of the Privacy Commissioner of Canada, "Draft OPC position on online reputation," OPCC, Jan. 26, 2018. [Online]. Available: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/pos_or_201801/

[40] N. Gladstone, "How facial recognition technology permeated everyday life," Centre for International Governance Innovation, Sept. 19, 2018. [Online]. Available: https://www.cigionline.org/articles/how-facial-recognition-technology-permeated-everyday-life

[41] R. Cohen, "School insecurity," *Democracy Journal,* Dec. 10, 2019. [Online]. Available: https://democracyjournal.org/magazine/school-insecurity/.

[42] K. Miles, "Should colleges really be putting smart speakers in dorms?" *MIT Technology Review,* Dec. 27, 2019. [Online]. Available: https://www.technologyreview.com/s/614937/colleges-smart-speakers-in-dorms-privacy/

[43] C. Horgan, "Spying on kids to prevent school shootings will backfire," *GEN,* Oct. 30, 2019. [Online]. Available: https://gen.medium.com/policing-students-texts-is-a-great-way-to-destroy-all-trust-2aedeac44411

[44] Internet Society, *Canadian Multistakeholder Process: Enhancing IoT Security – Final Outcomes and Recommendations Report,* May 28, 2019. [Online]. Available: https://iotsecurity2018.ca/draft-outcomes-report/

[45] C. Kang, "Toymaker VTech settles charges of violating child privacy law," *The New York Times,* Jan. 8, 2018. [Online]. Available: https://www.nytimes.com/2018/01/08/business/vtech-child-privacy.html.

[46] C. Warzel and S. Thompson, "Where even the children are being tracked," *The New York Times,* Dec. 21, 2019. [Online]. Available: https://www.nytimes.com/interactive/2019/12/21/opinion/pasadena-smartphone-spying.html

[47] A. Speri, "The NYPD kept an illegal database of juvenile fingerprints for years," *The Intercept,* Nov. 13, 2019. [Online]. Available: https://theintercept.com/2019/11/13/nypd-juvenile-illegal-fingerprint-database/

[48] A. Cavoukian, "Privacy by design: The 7 foundational principles," Information and Privacy Commissioner of Ontario, Jan. 2011. [Online]. Available: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

[49] Consumer Protection: *Privacy by Design for Consumer Goods and Services,* ISO/PC 317, International Standards Organization, Geneva, Switzerland. [Online]. Available: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/committee/69/35/6935430.html (accessed Jan. 7, 2020).

[50] B. Zimmer, *Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act – Report of the Standing Committee on Access to Information, Privacy and Ethics,* House of Commons, Canada, Feb. 2018. [Online]. Available at: https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9690701/ethirp12/ethirp12-e.pdf

[51] "Mattel Children's Privacy Statement," Mattel. [Online]. Available: https://www.mattel.com/en-us/childrens-privacy-statement (accessed Jan. 7, 2020).

[52] M. Johnson, "How do Canadian teens make decisions when sharing photos?" MediaSmarts Blog, Apr. 19, 2017. [Online]. Available: http://mediasmarts.ca/blog/how-do-canadian-teens-make-decisions-when-sharing-photos

[53] U. Benloiel and S. Blecher, "The duty to read the unreadable," *Boston Coll. Law Rev.,* vol. 60, no. 2225, Jan. 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3313837

[54] 5Rights Foundation, "Standard for an age appropriate digital services framework." [Online]. Available: https://5rightsfoundation.com/our-work/design-of-service/standard-for-an-age-appropriate-digital-services-framework.html. (accessed Jan. 7, 2020).

[55] "Government to strengthen security of internet-connected products," GOV.UK, Jan. 27, 2020. [Online]. Available: https://www.gov.uk/government/news/government-to-strengthen-security-of-internet-connected-products

[56] C. Jee, "Instagram has started asking new users for their birthdays," *MIT Technology Review,* Dec. 5, 2019. [Online]. Available: https://www.technologyreview.com/f/614845/instagram-has-started-asking-new-users-for-their-birthdate/

[57] S. O'Hear, "Digital identity startup Yoti raises additional £8M at a valuation of £82M," *TechCrunch,* Aug. 2, 2019. [Online]. Available: http://social.techcrunch.com/2019/08/02/yoti/

[58] J. Waterson, "UK drops plans for online pornography age verification system," *The Guardian,* Oct. 16, 2019. [Online]. Available: https://www.theguardian.com/culture/2019/oct/16/uk-drops-plans-for-online-pornography-age-verification-system

[59] OECD, "The protection of children online: Recommendations of the OECD Council – Risks faced by children online and policies to protect them," OECD Digital Economy Papers #179, OECD Publishing, Paris, France, May 2, 2011. [Online]. Available: https://doi.org/10.1787/5kgcjf71pl28-en

[60] S. Livingstone, L. Kirwil, and E. Staksrud, "In their own words: What bothers children online?" London School of Economics and Political Science, Feb. 2013. [Online]. Available: https://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/Intheirownwords020213.pdf

[61] Public Safety Canada, "Public Safety Canada announces expansion of National Strategy for the Protection of Children from Sexual Exploitation on the Internet," Government of Canada, Aug. 6, 2019. [Online]. Available: https://www.canada.ca/en/public-safety-canada/news/2019/08/public-safety-canada-announces-expansion-of-national-strategy-for-the-protection-of-children-from-sexual-exploitation-on-the-internet0.html

[62] Canadian Centre for Child Protection, "Child Sexual Abuse Images in the Internet: A Cybertip.ca Analysis," CCCP, Jan. 2016. [Online]. Available: https://protectchildren.ca/en/resources-research/child-sexual-abuse-images-report/

[63] Canadian Centre for Child Protection, "How we are failing children: Changing the paradigm," CCCP, 2019. [Online]. Available: https://protectchildren.ca/en/resources-research/child-rights-framework/

[64] J. W. Patchin, "Sextortion: More insight into the experiences of youth," Cyberbullying Research Center, Nov. 19, 2019. [Online]. Available: https://cyberbullying.org/sextortion-more-insight-into-the-experiences-of-youth

[65] L.-D. Nuria, "Understanding grooming discourse in computer mediated environments," *Discourse Context & Media,* vol. 12, pp. 40–50, Jun. 2016, https://doi.org/10.1016/j.dcm.2016.02.004.

[66] A. Pascual and K. Marchini, "2018 child identity fraud study," Javelin Strategy and Research, Apr. 2018. [Online]. Available: https://www.javelinstrategy.com/coverage-area/2018-child-identity-fraud-study

[67] Identity Theft Resource Center, "The impact of identity theft on foster youth," ITRC, 2018. [Online]. Available: https://www.idtheftcenter.org/wp-content/uploads/2019/01/ITRC_dec18_white-pages-foster-youth_FINAL_web.pdf

[68] S. Coughlan, "'Sharenting' puts young at risk of fraud," *BBC News,* May 21, 2018. [Online]. Available: https://www.bbc.com/news/education-44153754

[69] M. Anderson, "A majority of teens have experienced some form of cyberbullying," Pew Research Center: Internet, Science & Tech, Sept. 27, 2018. [Online]. Available: https://www.pewresearch.org/internet/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/

[70] L. Ha, "A snapshot of cyberbullying," *Victims of Crime Research Digest,* Issue No. 7, 2014. [Online]. Available: https://www.justice.gc.ca/eng/rp-pr/cj-jp/victim/rd7-rr7/p2.html

[71] A. John et al., "Self-harm, suicidal behaviours, and cyberbullying in children and young people: Systematic review," *J. Med. Internet Res.,* vol. 20, no. 4, p. e129, 2018, doi: 10.2196/jmir.9044.

[72] "An update to our harassment policy," YouTube Official Blog, Dec. 11, 2019. [Online]. Available: https://youtube.googleblog.com/2019/12/an-update-to-our-harassment-policy.html

[73] "More updates on our actions related to the safety of minors on YouTube," YouTube Creator Blog, Feb. 28, 2019. [Online]. Available: https://youtube-creators.googleblog.com/2019/02/more-updates-on-our-actions-related-to.html

[74] T. Milosevic, "Social media companies' cyberbullying policies," *Int. J. Commun.,* vol. 10, pp. 5164–5185, Oct. 2016, https://ijoc.org/index.php/ijoc/article/view/5320/1818

[75] I. von Behr, A. Reding, C. Edwards, and L. Gribbon, "Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism," Rand Europe, 2013. [Online]. Available: https://www.rand.org/pubs/research_reports/RR453.html

[76] Canadian Security Intelligence Service, "2018 CSIS Public Report," Ottawa, ON, CAN: Public Works and Services Canada, Jun. 2019. [Online]. Available: https://www.canada.ca/content/dam/csis-scrs/documents/publications/2018-PUBLIC_REPORT_ENGLISH_Digital.pdf

[77] "How does ISIS try to recruit Canadian girls? By using same tactics as pedophiles, TV special says," *National Post,* Mar. 14, 2015. [Online]. Available: https://nationalpost.com/news/isis-recruiting-tactics-are-pretty-creepy

[78] J.T. Darden, *Tackling Terrorists' Exploitation of Youth,* American Enterprise Institute, May 2019. [Online]. Available: https://www.un.org/sexualviolenceinconflict/wp-content/uploads/2019/05/report/tackling-terrorists-exploitation-of-youth/Tackling-Terrorists-Exploitation-of-Youth.pdf

[79] Public Safety Canada, *National Strategy on Countering Radicalization to Violence,* Government of Canada, 2018. [Online]. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-strtg-cntrng-rdclztn-vlnc/index-en.aspx

[80] M. Ingram, "The YouTube 'radicalization engine' debate continues," *Columbia Journalism Review,* Jan. 9, 2020. [Online]. Available: https://www.cjr.org/the_media_today/youtube-radicalization.php

[81] "The four Rs of responsibility, part 1: Removing harmful content," YouTube Official Blog, Sept. 3, 2019. [Online]. Available: https://youtube.googleblog.com/2019/09/the-four-rs-of-responsibility-remove.html

[82] "The four Rs of responsibility, part 2: Raising authoritative content and reducing borderline content and harmful misinformation," YouTube Official Blog, Dec. 3, 2019. [Online]. Available: https://youtube.googleblog.com/2019/12/the-four-rs-of-responsibility-raise-and-reduce.html

[83] J. Cox and S. Cole, "How hackers are breaking into Ring cameras," *Vice,* Dec. 11, 2019. [Online]. Available: https://www.vice.com/en_ca/article/3a88k5/how-hackers-are-breaking-into-ring-cameras

[84] S. Antal, "What parents should know about Snapchat's augmented reality features," Family Online Safety Institute, Jun. 25, 2019. [Online]. Available: https://www.fosi.org/good-digital-parenting/what-parents-should-know-about-snapchats-augmented-reality-features/

[85] L. Kelion, "TikTok suppressed disabled users' videos," *BBC News,* Dec. 3, 2019. [Online]. Available: https://www.bbc.com/news/technology-50645345

[86] A. Tait, "Sarahah and tbh: inside the teenage obsession with anonymous apps," NewStatesmanAmerica, Sept. 27, 2017. [Online]. Available: https://www.newstatesman.com/2017/09/sarahah-and-tbh-inside-teenage-obsession-anonymous-apps

[87] Child Dignity Alliance, "Child Dignity Alliance Technical Working Group Report," [Online]. Available: https://www.inhope.org/media/pages/the-facts/download-our-whitepapers/135698579-1574371755/child-dignity-alliance-technology-working-group-report.pdf (accessed Feb. 28, 2020).

[88] Interagency Working Group on Sexual Exploitation of Children, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse,* Bangkok, Thailand: ECPAT International, Jun. 2016. [Online]. Available: https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---ipec/documents/instructionalmaterial/wcms_490167.pdf

[89] Department of Justice, "Cyberbullying and the non-consensual distribution of intimate images," Government of Canada, Jun. 2013. [Online]. Available: https://www.justice.gc.ca/eng/rp-pr/other-autre/cndii-cdncii/

[90] UK Public General Acts, "Sexual Offences Act 2003," legislation.gov.uk. [Online]. Available: https://www.legislation.gov.uk/ukpga/2003/42/section/15A (accessedJan. 13, 2020).

[91] Boys and Girls Clubs of Canada, "Responding to cyberbullying: House of Commons Standing Committee on Justice and Human Rights: Submission to study of Bill C-13, April 2014," BGCC, 2014. [Online]. Available: https://www.bgccan.com/index.php?securefile=2017/03/Responding-to-Cyberbullying-BGCCs-brief-on-Bill-C-13-2014.pdf

[92] Public Safety Canada, "Countering online child sexual exploitation: Sharing knowledge, enhancing safety – closed consultation," Government of Canada, Mar. 26, 2018. [Online]. Available: https://www.canada.ca/en/services/policing/police/consultation-countering-online-child-sexual-exploitation.html

[93] O. Solon, "Microsoft launches tool to identify child sexual predators in online chat rooms," *NBC News,* Jan. 9, 2020. [Online]. Available: https://www.nbcnews.com/tech/tech-news/microsoft-launches-tool-identify-child-sexual-predators-online-chat-rooms-n1112881

[94] J. Rubinstein and L. Fernandez, "The digital world is a dark, dangerous place for children – here's how we can change that," *World Economic Forum,* Nov. 29, 2019. [Online]. Available: https://www.weforum.org/agenda/2019/11/internet-safer-for-children-web-parents-digital/

[95] Susanna Greijer and Jaap Doe, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse.* Luxembourg: ECPAT, Jun. 2016. [Online]. Available: http://luxembourgguidelines.org/english-version/

[96] "University of Skövde," World Childhood Foundation, Sep. 14, 2018. [Online]. Available: https://childhood.org/this-is-childhood/projects/university-of-skovde/

[97] T. Burns and F. Gottschalk, Eds., Educating 21st Century Children: *Emotional Well-Being in the Digital Age.* Paris, France: OECD Publishing, 2019.

[98] W. Craig, "Safer internet day: New research on the challenges of parenting in the digital age," TELUS, Feb. 4, 2019. [Online]. Available: https://www.telus.com/en/wise/resources/content/article/safer-internet-day-new-research-on-the-challenges-of-parenting-in-the-digital-age

[99] B. C. McHugh, P. Wisniewski, M. B. Rosson, and J. M. Carroll, "When social media traumatizes teens: The roles of online risk exposure, coping, and post-traumatic stress," *Internet Res.,* vol. 28, no. 5, pp. 1169–1188, Jan. 2018, doi: 10.1108/IntR-02-2017-0077.

[100] L. Matsakis, "TikTok Overhauls Community Guidelines to Ban 'Underage Delinquent Behavior," *Wired,* Jan. 8, 2020. [Online]. Available: https://www.wired.com/story/tiktok-overhauls-community-guidelines/

[101] S. Livingstone et al., "Children's online activities, risks and safety: A literature review by the UKCCIS Evidence Group," UK Council for Child Internet Safety, Oct. 2017. [Online]. Available: https://www.gov.uk/government/publications/childrens-online-activities-risks-and-safety-a-literature-review-by-the-ukccis-evidence-group

[102] S. Maheshwari, "On YouTube kids, startling videos slip past filters," *The New York Times,* Nov. 4, 2017. [Online]. Available: https://www.nytimes.com/2017/11/04/business/media/youtube-kids-paw-patrol.html

[103] J. Bridle, "Something is wrong on the internet," Medium, Jun. 21, 2018. [Online]. Available: https://medium.com/@jamesbridle/something-is-wrong-on-the-internet-c39c471271d2

[104] B. Popper, "YouTube says it will crack down on bizarre videos targeting children," *The Verge,* Nov. 9, 2017. [Online]. Available: https://www.theverge.com/2017/11/9/16629788/youtube-kids-distrubing-inappropriate-flag-age-restrict

[105] A. Marchant et al., "A systematic review of the relationship between internet use, self-harm and suicidal behaviour in young people: The good, the bad and the unknown," *PLOS ONE,* vol. 12, no. 8, p. e0181722, Aug. 2017, doi: 10.1371/journal.pone.0181722.

[106] J. Pitre, "We can't afford to be in the dark about digital self-harm – and its real-life consequences," *The Globe and Mail,* Mar. 22, 2019. [Online]. Available: https://www.theglobeandmail.com/opinion/article-we-cant-afford-to-be-in-the-dark-about-digital-self-harm-and-its/

[107] V. Steeves, *Young Canadians in a wired world, phase III: Encountering racist and sexist content online.* Ottawa, On, CAN: MediaSmarts, 2014. [Online]. Available: http://mediasmarts.ca/sites/mediasmarts/files/publication-report/full/ycwwiii_encountering_racist_sexist_content_online.pdf

[108] Ofcom, "Children and parents: Media use and attitudes report 2018," Ofcom, Feb. 21, 2019. [Online]. Available: https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2018

[109] B. Tynes, "Online racial discrimination: A growing problem for adolescents," *American Psychological Association,* Dec. 2015. [Online]. https://www.apa.org/science/about/psa/2015/12/online-racial-discrimination

[110] C. P. Society, "Digital media: Promoting healthy screen use in school-aged children and adolescents," Canadian Paediatric Society, Jun. 6, 2019. [Online]. Available: https://www.cps.ca/en/documents/position/digital-media

[111] J. Pinsker, "How should parents interpret screen-time recommendations?" *The Atlantic,* Apr. 29, 2019. [Online]. Available: https://www.theatlantic.com/family/archive/2019/04/who-screen-time-recommendations/588178/

[112] A. K. Przybylski, A. Orben, and N. Weinstein, "How much is too much? Examining the relationship between digital screen engagement and psychosocial functioning in a confirmatory cohort study," *J. Am. Acad. Child Adolesc. Psychiatry,* Aug. 7, 2019 [Online]. doi: 10.1016/j.jaac.2019.06.017.

[113] "Autism and Screen Time: Special brains, special risks," *Psychology Today,* Dec. 31, 2016. [Online]. Available: https://www.psychologytoday.com/blog/mental-wealth/201612/autism-and-screen-time-special-brains-special-risks

[114] A. C. Madrigal, "Raised by YouTube," *The Atlantic*, Oct. 2018. [Online]. Available: https://www.theatlantic.com/magazine/archive/2018/11/raised-by-youtube/570838/

[115] E. Aarseth et al., "Scholars' open debate paper on the World Health Organization ICD-11 Gaming Disorder proposal," *J. Behav. Addict.,* vol. 6, no. 3, pp. 267–270, Dec. 2016, doi: 10.1556/2006.5.2016.088.

[116] D. Heaven, "Video game addiction is now being recognized – what happens next?" MIT Technology Review, Nov. 25, 2019. [Online]. Available: https://www.technologyreview.com/s/614747/video-game-addiction-is-now-being-recognizedwhat-happens-next/

[117] "Social Media Councils: Consultation," ARTICLE 19, Jun. 11, 2019. [Online]. Available: https://www.article19.org/resources/social-media-councils-consultation/

[118] C. Bradley and R. Wingfield, "Content regulation laws threaten our freedom of expression. We need a new approach," Global Partners Digital, May 15, 2018. [Online]. Available: https://www.gp-digital.org/content-regulation-laws-threaten-our-freedom-of-expression-we-need-a-new-approach/

[119] F. McKelvey, H. Tworek, and C. Tenove, "How a standards council could help curb harmful online content," Policy Options, Feb. 11. 2019. [Online]. Available: https://policyoptions.irpp.org/magazines/february-2019/standards-council-help-curb-harmful-online-content/

[120] A. Chen, "The Human Toll of Protecting the Internet from the Worst of Humanity," The New Yorker, Jan. 28, 2017. [Online]. Available: https://www.newyorker.com/tech/annals-of-technology/the-human-toll-of-protecting-the-internet-from-the-worst-of-humanity

[121] D. Gilbert, "Facebook is forcing its moderators to log every second of their days — even in the bathroom," Vice, Jan. 9, 2020. [Online]. Available: https://www.vice.com/en_us/article/z3beea/facebook-moderators-lawsuit-ptsd-trauma-tracking-bathroom-breaks

[122] "Safety by Design," eSafety Commissioner. [Online]. Available: https://www.esafety.gov.au/key-issues/safety-by-design (accessed Dec. 3, 2019).

[123] S. Livingstone, "Children: A special case for privacy?" *Intermedia,* vol. 46, no. 2, pp. 18–23, Jul. 2018.

[124] B. Miller and S. Bherwal, "Policy Lab collaborates with young people to win the Cabinet Office Innovator Award 2019," Gov.UK Policy Lab, Jan. 13, 2020. [Online]. Available: https://openpolicy.blog.gov.uk/2020/01/13/policy-lab-collaborates-with-young-people-to-win-the-cabinet-office-innovator-award-2019/

[125] Office of the Privacy Commissioner of Canada, "Privacy law reform: A pathway to respecting rights and restoring trust in government and the digital economy," OPCC, Dec. 10, 2019. [Online]. Available: https://priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/

[126] J. Ling, "The Cyberbullying Bill Committee," *CBA/ABC National* [Online]. Available: https://www.nationalmagazine.ca/en-ca/articles/the-practice/new-law/2014/the-cyberbullying-bill-committee

CSA Group Research

In order to encourage the use of consensus-based standards solutions to promote safety and encourage innovation, CSA Group supports and conducts research in areas that address new or emerging industries, as well as topics and issues that impact a broad base of current and potential stakeholders. The output of our research programs will support the development of future standards solutions, provide interim guidance to industries on the development and adoption of new technologies, and help to demonstrate our on-going commitment to building a better, safer, more sustainable world.

CSA GROUP™

© 2020 Canadian Standards Association. All Rights Reserved.