STANDARDS RESEARCH

Children's Privacy in the Age of Artificial Intelligence

March 2021

Author

Jasmine Irwin, Springboard Policy
Alannah Dharamshi, Springboard Policy
Noah Zon, Springboard Policy

Project Advisory Panel

Brent Barron, Canadian Institute for Advanced Research

Cara Yarzab, Prodigy Game

Carol Todd, Amanda Todd Legacy Society

Fardouz Hosseiny, Centre of Excellence on PTSD

Gareth Jones, Canada Safety Council

Matthew Johnson, MediaSmarts

Nimmi Kanji, TELUS Social Purpose Programs

Uyen Ta, Mental Health Commission of Canada

Valerie Steeves, University of Ottawa

Wendy Craig, PrevNET

Hélène Vaillancourt, CSA Group

Nicki Islic, CSA Group (Project Manager)

Financial Support

This CSA Group research report was prepared with financial support from the Office of the Privacy Commissioner of Canada's (OPC) Contributions Program.

Disclaimer

Table of Contents

Glossary 5

Executive Summary 6

Introduction 8

About the Report 9

1 The Need for a Child-Specific Approach 9

1.1 Children are *Deeply* Affected by AI 10

1.1.1 Children and AI in Homes 11

1.1.2 Children and AI in Schools and Learning Environments 11

1.1.3 Children and AI in Public Services and Spaces 12

1.2 Children are *Distinctly* Affected by AI 12

1.2.1 AI and Children's Privacy Needs 12

1.2.2 AI and Children's Privacy Circumstances 13

2 Risks to Children's Privacy 14

2.1 Data Risks 14

2.1.1 Magnitude of Data 14

2.1.2 Sensitivity of Data 15

2.1.3 Selling and Sharing of Data 15

2.1.4 Lifespan of Data 16

2.2 Function risks 16

2.2.1 Data Inference and Re-Identification Functions 16

2.2.2 Surveillance Functions 16

2.2.3 Profiling Functions 17

2.2.4 Decision-Making Functions 17

2.3 Oversight Risks 17

2.3.1 Fairness 17

2.3.2 Transparency and Explainability 18

2.3.3 Accountability 18

3 Recommendations to Promote Children's Privacy 18
3.1 Before Deployment: Design and Development of AI Systems 19
3.1.1 Mandate and Operationalize Children's Privacy by Design 19
3.1.2 Require Children's Privacy Impact Assessments 20
3.2 During Adoption: User Privacy and Choice 20
3.2.1 Develop Educational Resources for Children, Teachers, and Parents 20
3.2.2 Require Child-Friendly Notices and Terms of Service 21
3.2.3 Encourage Certification and Consumer Labelling 22
3.2.4 Provide Cynamic and Granular Consent Options 22
3.3 After Use: Oversight and Accountability 23
3.3.1 Mandate Organizational Oversight Mechanisms 23
3.3.2 Fund Independent Oversight Institutions 23
3.3.3 Introduce Strict Penalties for Privacy Violations 23
Conclusion 24
Acknowledgements 25
References 26

Glossary

This glossary outlines how the following terms are used in this report.

Artificial Intelligence (AI)

AI broadly refers to a machine-based system that, given a defined set of objectives, can perform tasks normally considered to require human intelligence such as predictions and decisions [1], [2]. In this report, machine learning, data processing, and algorithmic decision-making are all referenced under the umbrella of AI.

Internet of Things (IoT)

IoT refers to the networking of physical objects that connect and exchange data with other devices and systems over the Internet [3]. It includes objects such as Internet-connected smart toys, smart home hubs, and smart phones.

Online platform

An online platform is a digital service that facilitates interactions between two or more users over the Internet [4]. It includes digital services such as marketplaces, search engines, and social media.

Children

Unless otherwise stated, the term children in this report is used to refer to people under the age of 18 [5].

Executive Summary

Artificial intelligence (AI) is playing a growing role in children's lives, fundamentally reshaping their everyday experiences and places – from their homes, to their schools, to other public services and spaces. While the application of AI has rapidly expanded, the tools to address the challenges AI can pose to children's privacy have not kept pace.

Instead, children are navigating the age of AI with little consideration for their best interests from developers and policymakers alike. But children are *deeply* affected by AI; they both directly and indirectly interact with AI-enabled technologies, including those designed for adults. Children are also *distinctly* affected by AI; they have specific privacy rights, needs, and circumstances that are impacted by this technology.

There is an immediate need for policymakers to address this gap and develop a child-specific approach to privacy in the context of AI. If left unaddressed, this oversight will have profound implications for present and future generations of children.

This report seeks to advance understanding and protections of children's privacy by focusing on three main areas of risk from AI:

- **Data risks:** AI requires data to learn and improve, incentivizing the mass collection of data. The sheer magnitude and scope of data collected about children today is unprecedented. Children's data captured and processed by AI systems may include sensitive information. This data can be shared or sold to third parties and may follow children over the course of their lives.
- **Function risks:** AI applications often use data in ways that infringe on children's privacy and autonomy. AI functions like surveillance, profiling, decision-making, and inference are already commonly used in children's lives, generally in "low-stakes" applications like targeted online ads. However, AI functions are increasingly being deployed in "high-stakes" applications like university admissions, child protective services, and biometric monitoring.
- **Oversight risks:** AI can produce unfair, incorrect, or discriminatory outcomes for children using their personal information. The complexity of AI can prevent humans from easily understanding or contesting how these algorithmic decisions are made. A lack of formalized governance or common standards for AI means that those who create, deploy, or profit from AI systems are currently subject to minimal transparency and accountability requirements.

Used responsibly, AI technology has remarkable potential to improve the lives of children. However, without effective interventions, the risks to children's privacy from AI may have profound negative impacts on children's present and future lives.

To address the challenges AI poses to children's privacy, this report identifies a number of recommended interventions. Some of these actions are cross-cutting and involve commitments to meaningfully and systematically include children in the development of AI and privacy policies that affect their lives. Others are targeted at specific stages across the lifecycle of AI – from integrating children's privacy considerations before technologies are deployed, to increasing their capacity to make informed privacy decisions, to ensuring they have mechanisms to pursue redress for any harms.

While these recommendations cannot eliminate all the potential risks to children, they represent important steps in promoting their privacy in the age of AI. A summary of recommendations is presented in Table E1.

Table E1: Summary of Recommendations

Cross-Cutting Actions		
Consider children as a distinct and vulnerable population		
Involve children in privacy and AI policy development		
Interventions Across the Life Cycle of AI		
Before Deployment	**During Adoption**	**After Use**
Mandate and operationalize children's privacy by design	Develop educational resources for children, teachers, and parents	Mandate organizational oversight mechanisms
Require children's privacy impact assessments	Require child-friendly notices and terms of service	Fund independent oversight institutions
	Encourage certification and consumer labelling	Introduce strict penalties for privacy violations
	Provide dynamic and granular consent options	

"Some of the most significant implications rest beneath the surface, in the ways that AI captures, stores, and uses data generated by familiar routines in children's day-to-day lives."

Introduction

The role that artificial intelligence (AI) is playing in society is growing, with increasing impact on the lives of children. The COVID-19 pandemic has accelerated this digital transition. Starting in 2020, the realities of social distancing shifted even more of children's activities online – from learning to play to health care – prompting rapid and widespread adoption of AI-enabled technologies. These changes are significant. The rise of AI has the potential to make children's lives more convenient and in some cases more equitable [6], [7]. However, AI also poses substantial risks to children's privacy – risks that are underexplored and underregulated.

Some of the new experiences for children that come with AI are highly visible. It is remarkable that children today can "talk" to smart toys alongside their imaginary friends. However, some of the most significant implications rest beneath the surface, in the ways that AI captures, stores, and uses data generated by familiar routines in children's day-to-day lives. School photos that are shared over the Internet, rather than through the mail, can be analyzed and used to identify individuals through facial recognition technology. Curious children who ask a smart speaker, rather than a parent, for information are not just teaching themselves but are also teaching AI to recognize their voices. Algorithmic grading means that a poor grade on just one math test is not just a normal part of learning but could be used as a data point to predict a child's future performance and opportunities.

This "datafication" of growing up and increasing application of AI is not inherently harmful. But it raises a number of privacy concerns:

- AI can expand the magnitude of data that can be collected about children, generating potentially sensitive information that follows them into adulthood;
- AI can use children's information to make decisions about them that impact what content they see and what opportunities they can access; and
- AI can lack transparency and be difficult to understand and explain, making it hard to ascertain how children's information is used or to ensure accountability.

Despite these risks, policy responses have been largely adult-centric, dedicating little attention to the deep and distinct impact of AI on children. For instance, proposed modernized privacy legislation, introduced by the Canadian government in 2020, mentioned minors only once in its 124 pages [8]. Children were not mentioned at all.

This lack of a child-specific AI and privacy policy is a significant oversight. Children are early adopters of AI-enabled technologies and have distinct privacy rights and needs that necessitate attention to their evolving capacities and best interests. Yet they are interacting with AI systems designed and deployed with adult users in mind. There is an urgent need for decision-makers to consider impacts on children's privacy

and develop interventions that reflect the AI world of children today and tomorrow.

This report seeks to address this gap by exploring the critical challenges that are emerging and by providing recommendations on promoting children's privacy in the age of AI. As presented in Figure 1, the report outlines the need for a child-specific approach and identifies three major areas in which AI poses risks to children's privacy: data risks, function risks, and oversight risks. It then explores how these risks can be reduced with recommended responses across the life cycle of AI systems: before deployment, during adoption, and after use.

About the Report

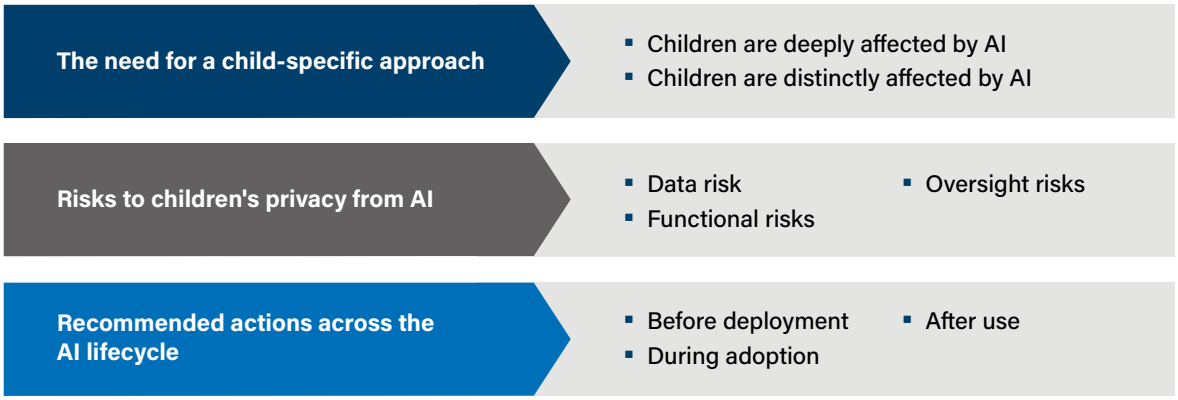
This research report builds on CSA Group's previous publication, *Children's Safety and Privacy in the Digital Age,* and narrows the focus on special considerations for children's privacy in the context of AI [9]. It was developed with generous support from the Office of the Privacy Commissioner of Canada's (OPC) Contributions Program. The analysis draws on a review of academic and grey literature, environmental scans of industry standards and government approaches, a workshop with 27 participants, and three research interviews. Both the workshop and interviews were held in the fall of 2020 and were conducted on a background basis to allow individuals to speak freely and openly.

1 The Need for a Child-Specific Approach

Governments and organizations across the globe have recognized both the opportunities and the elevated privacy risks posed by digital technologies, including AI, and are beginning to address these issues. For instance, in 2017, Canada published the first national AI strategy in the world and since then over 25 other countries have released their own strategies [10]. There has also been a wave of data protection and privacy reforms, with 30 countries enacting new statutes or amending existing legislation in the past two years alone [11]. Most notably, the European Union's *General Data Protection Regulation* (GDPR) has emerged as one of the most comprehensive privacy laws, heavily influencing other jurisdictions [12].

Canada's Information and Privacy Commissioners have also called for the modernization of privacy protections [13]. Recently, the Office of the Privacy Commissioner of Canada (OPC) considered the privacy risks of AI and delivered recommendations for updating the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Canada's federal consumer privacy law [14]. PIPEDA was passed in 2000, a time when social media sites were in their infancy and Netflix videos came in the mail, and it is poorly equipped to respond to today's AI realities [15]. In response to these challenges, new

Figure 1: Overview of discussion on children's privacy in the age of AI



draft legislation to implement Canada's recent Digital Charter has been introduced under Bill C-11, which, if passed, would enact the *Consumer Privacy Protection Act* (CPPA) and the *Personal Information and Data Protection Tribunal Act* [8]. Similarly, the Government of Canada initiated a review of the *Privacy Act,* which governs personal information held by the federal government, with a view to AI and other emerging technologies [16].

While these developments are important steps towards privacy promotion in the age of AI, current efforts largely neglect the rights, needs, and circumstances of children – despite the fact that they make up a third of all online users [17].

Across the board, policy development that considers children's rights in the digital age is immature. A recent review by the United Nations Children's Fund (UNICEF) of 20 national AI strategies has revealed minimal engagement with the impact of AI on children, including in the area of data and privacy protection [10]. Canada's strategy has no meaningful mention of children [18]. Similarly, while proposed updates to Canadian federal privacy legislation consider many risks from AI, the changes do not account for children's distinct rights, needs, and circumstances.

Only a few recent efforts have given specific attention to children in the context of AI, including UNICEF's Generation AI initiative [19] and *Policy Guidance on AI for Children* [6], and the Beijing Academy of Artificial Intelligence's *Artificial Intelligence for Children: Beijing Principles* [20]. Further and immediate action is needed to address this critical gap in policy. As indicated in Figure 2, targeted attention to children's privacy is needed for two reasons: children are both *deeply* and *distinctly* affected by AI.

1.1 Children are *Deeply* Affected by AI

Children's everyday lives are increasingly mediated, both directly and indirectly, by AI-powered technologies. This impact is not only limited to systems meant specifically for their demographic. For instance, a 2020 survey showed that 71% of current smart speaker owners with children under 18 said they wanted to buy another smart speaker to entertain their children, an increase from 47% in 2019 [21].

Children also rapidly adopt new technologies designed for adults-by-default [6]. Although some child-specific models of popular technologies exist, children routinely use adult versions. Gaining access by "fooling" age verification systems is typically a simple task – as easy as checking a box or changing a year in a birthdate [22]. Even when children do not directly seek out these technologies, they may still be indirectly interacting with them because of the spread of AI where they live, learn, and play.

Both child-specific and adult-by-default AI systems can be found across the key spaces of children's lives – from their homes, to their schools, to other public services and spaces – with potential impacts on their privacy [23]. This trend has only been accelerated by the COVID-19 pandemic, which in 2020 rapidly caused transitions to digital variations of many children's activities.

Figure 2: The need for a child-specific approach to privacy in the age of AI

1.1.1 Children and AI in Homes

Homes are typically where we expect to have the most privacy for ourselves and our children, but consumer products and services commonly used in private lives are increasingly being embedded with AI [24]. As a result, children's personal lives, from play, to leisure, to social connection, are being tracked, analyzed, and even shared in novel ways [25]. These AI technologies break boundaries between private, public, and commodifiable information and experiences.

For instance, Internet-connected smart toys use AI to provide personalized and interactive play experiences but may analyze and store children's voices, prompt disclosure of personal information, and be vulnerable to hacking or data breaches [26], [27]. Other Internet of Things (IoT) technologies like smart speakers use AI to create convenience but capture home life data, intertwining and processing children's information with that of adults in a household [28]. Online platforms such as TikTok and YouTube also use AI to recommend and mediate content based on individualized information, with some experts arguing that these algorithms may be creating echo-chambers of radicalization and disinformation [29]. Many of these popular online platforms also share data, including that of children, with third parties [23].

1.1.2 Children and AI in Schools and Learning Environments

Schools and other learning environments are another central space in children's lives where AI-enabled technologies have an increasing role. As a result, students' activities, behaviour, and even emotions are being monitored, profiled, evaluated, and shared [33]. These tools are typically developed and supplied by private vendors, which raises concerns about the potential commercialization of students' data and associated privacy risks if information is used for supplementary purposes [34].

For instance, AI-enabled personalized learning systems can provide lesson plans tailored to each child's needs and abilities but may lack transparency on how their data are generated, shared, and used [35]. Similarly, grading and admissions tasks are also being streamlined with AI but may opaquely use children's information to make critical decisions that impact their access to future opportunities and life trajectories [36]. Surveillance systems may also be using AI to enhance and expand monitoring of students for safety and conduct violations in both online and physical contexts. These systems may collect sensitive information, infringe on anonymity, and criminalize differences in behaviour in biased and discriminatory ways [32], [37].

Examples of AI in Children's Homes

- **Hello Barbie** is an interactive doll that records children's voices and sends this information over the Internet for analysis by AI, which creates an appropriate response [30]. Researchers have found that the doll may prompt disclosure of personal information and can be easily hacked, potentially allowing access to stored audio recordings and even the doll's microphone [30]. While caregivers can listen to their children's recordings and delete personal information, this feature is onerous and unrealistic for many parents, and may also interfere with children's need for relational or play privacy from their parents [31].
- **YouTube** uses AI to track search histories, device identifiers, location, and other personal data of users in order to recommend content that will maximize time spent on the site and to target advertising [23]. While there is a new child-specific version, YouTube Kids, which has some stronger privacy practices, children still predominantly use the adult platform [32].

"Healthy childhood development depends on privacy. It is what enables children to tackle challenges, make mistakes, explore their identities, and move through other critical experiences of growing up."

1.1.3 Children and AI in Public Services and Spaces

AI technologies can also be found in other public services and spaces that children access. As a consequence, even if children, parents, or teachers were able to make informed privacy-preserving choices at home and school, the fact that children use a wide range of public services, move through shared public spaces, and are subject to government decision-making means that their information can be captured and used by AI without much of their own choice in the matter.

For instance, AI is being incorporated into health care, including pediatric care [41]. Alongside the data they produce as patients, children may also generate health-related data through the burgeoning AI-enabled wellness industry, including wearables and health trackers [42].

AI can also be found in child protective service systems and criminal justice systems for the express purpose of protecting children. However, these applications may simultaneously facilitate harm by collecting sensitive information and using it in biased algorithms that further embed discrimination without meaningful transparency, explanation, or redress [43], [44]. Even as children move through public spaces – shopping at the mall, walking through their neighbourhood, going through customs at the airport – they may be visible to AI technologies that can view, track, and identify biometric markers, such as through facial recognition [45].

1.2 Children are *Distinctly* Affected by AI

In addition to the deep and widespread impact of AI on children's lives, it also has distinct implications for their rights and needs that are fundamental to growing up. That is why in addition to their general human rights, children's distinct right to privacy is highlighted in the *UN Convention on the Rights of the Child* (CRC) [5] and in emerging children's digital rights frameworks such as the 5Rights Framework [49]. Child privacy rights reflect their more limited legal options as minors, their ongoing development needs, and their heightened malleability and potential vulnerability to harm [17]. In turn, protecting children's privacy depends on a more proactive effort to consider their best interests and evolving capacities [50], [51].

1.2.1 AI and Children's Privacy Needs

Healthy childhood development depends on privacy. It is what enables children to tackle challenges, make mistakes, explore their identities, and move through other critical experiences of growing up [52]. It is also an enabler of many other children's rights, including their right to non-discrimination, right to freedom of expression, and right to freedom of association and assembly [53], [54].

Research demonstrates that children value privacy in digital spaces and want to have agency in controlling who knows their information, how it is processed, and for what purposes [55]. While children's development

is multifaceted, their desire for agency in privacy preservation and capacity for informed decision-making generally increases as they grow up [55]. As they transition through adolescence, children may also both need and want privacy not just from external actors but also within their own families [56]. For instance, children may need privacy from their parents or guardians in order to develop and freely explore their sexuality, political views, and religious beliefs [51].

Children by nature are also more susceptible to some of the invasive features of AI. For instance, the use of AI in online platforms to "nudge" or "hack" human behaviour (e.g., maximize time spent on an online platform, increase the likelihood of personal information disclosure) has elevated significance when considering the potential impacts on the ongoing development and identity-construction of children [57], [58]. Infringements on children's privacy by AI may also carry over to their adult lives, potentially impacting their future employment, relationships, and financial inclusion [51].

1.2.2 AI and Children's Privacy Circumstances

Children's capacity and conditions for exercising their privacy are different than adults. Children may lack the awareness or have limited literacy skills with which to fully grasp their right to privacy and understand the risks and potential long-term impacts of data sharing and AI processing [59]. While children are generally tech-savvy and want to preserve their privacy, they tend to have a narrower and less critical conception of digital privacy [60]. Children tend to think of privacy in *interpersonal* ways or between themselves and other individuals or groups. They struggle (as do most adults) to understand their privacy in more abstract, commercial, or institutional terms – like how their data are traced or inferenced by AI – and therefore have limited capacity to assess associated risks [55]. The "black box" of AI further obscures the connections between inputs and outcomes, making privacy risk assessment even more difficult for children.

Examples of AI in Children's Schools and Learning Environments

- **Proctorio** is an exam proctoring software that has proliferated in the transition to online education during COVID-19. It uses AI to turn students' computers into remote exam supervisors by surveilling them through their webcams, microphones, and keyboards and flagging behaviours it deems suspicious for review by the class instructor [38]. Critics of this software argue that it violates students' privacy and is likely to flag marginalized students unequally, including on the basis of race, disability, and income, due to bias and inaccuracy in "abnormality" detection [38].
- **The International Baccalaureate Organization (IBO)** opted to use an algorithm to determine students' grades when COVID-19 forced the cancellation of in-person exams. This algorithm used students' past coursework scores, information from teachers, and schools' historic results to predict what students "would have" scored if they had written the final exam [39]. Many students received grades that differed substantially from their past performance, without meaningful explanation or adequate redress, which in some cases resulted in lost scholarships and revoked admission to post-secondary institutions [40].

Children's privacy circumstances also differ due to the mediating role of caregivers in their interactions with AI systems and privacy decisions. Parents or guardians are commonly tasked with providing consent on behalf of children below a certain age [61]. However, relying on parents to exercise children's privacy can be problematic and impractical. Parents may have different interests and privacy preferences than their children but retain significant authority in choices on how their information is shared and used [62]. Parental involvement in protection may also undermine children's need for privacy from their parents in some instances, and needs to be considered in balance with children's evolving capacity to take agency in their privacy decisions [63]. At the same time, the parental consent approach may also shift the burden of responsibility for privacy harms away from the developers and purveyors of AI systems.

Examples of AI in Children's Public Services and Spaces

- **Cadillac Fairview Malls** embedded facial recognition technology in the wayfinding directories of Canadian malls to analyze visitors' images without obtaining proper consent [46]. The AI tool captured faces and converted them into a "biometric numerical representation" of each individual and this information was used to assess the age, gender, and movement of shoppers, potentially including children [47].
- **Allegheny Family Screening tool** is an algorithmic decision support system used for child protection in Allegheny, Pennsylvania. The algorithmic tool uses data to identify and flag children at high risk for abuse or neglect and informs decisions about when authorities should intervene or investigate [48].

2 Risks to Children's Privacy

Children's privacy is multifaceted; it includes their ability to control their data, move through spaces with autonomy, communicate without interception, and make independent decisions [64]. It is also highly contextual and relational; children's privacy preferences consist of multiple considerations, including what about their private lives is known, by whom, for what purposes, and with what consequences [41].

By collecting their data and inputting the information into algorithms to achieve different functionalities with limited oversight, AI may pose potential risks to all these aspects of children's privacy. As shown in Figure 3, there are three main categories of risk to children's privacy from AI: data risks, function risks, and oversight risks.

2.1 Data Risks

One of the fundamental risks to children's privacy from AI stems from its reliance on data for algorithmic training, testing, and ongoing functionality. These data may be particularly sensitive, accessed by different actors, and used for long timeframes and diverse purposes, consequently posing risks to children's privacy.

2.1.1 Magnitude of Data

AI expands the magnitude of data collected about children. These systems generate large volumes of data, and in some cases do so beyond what is necessary for system functionality [65]. In order to use AI technologies, children (or their guardians) often have to agree to this sweeping data collection through dense and unintelligible terms of service that do not promote meaningful consent [66], [67]. Some workshop experts noted that children are beginning to accept this quid pro quo of data in exchange for access as a normal practice.

Similarly, AI diversifies the variety of data collected about children, expanding the kinds of experiences and behaviours that can be datafied. These systems not only collect information that children knowingly disclose but also generate vast amounts of other data points that are not explicitly shared. For instance, AI can collect data traces or "footprints" children leave

Figure 3: Categories of risk to children's privacy from AI technologies

Data Risks	Function Risks	Oversight Risk
▪ Magnitude of data ▪ Sensitivity of data ▪ Selling and sharing of data ▪ Lifespan of data	▪ Data inference and re-indentification functions ▪ Surveillance functions ▪ Profiling functions ▪ Decision-making functions	▪ Fairness ▪ Transparency and explainability ▪ Accountability

behind as they explore digital spaces, such as browser cookies [55]. Children's data can also be generated through the use of AI-enabled technologies by parents, peers, other caregivers, and even strangers [68].

2.1.2 Sensitivity of Data

AI systems may collect particularly personal and sensitive data about children that identify them as individuals and connect them to particular groups, such as data on age, gender, and ethnicity [69]. These technologies also frequently collect children's names, dates of birth, and home addresses – all key information that is used in identity theft and fraud [70]. Other AI applications, such as facial recognition, collect biometric data that are unique to each child, potentially further compromising the security of their identities and undermining their ability to ever be anonymous again [51]. In other cases, the design of some AI interfaces, such as smart toys and chat bots, may prompt children to volunteer particularly personal information about themselves by encouraging the development of trusting relationships with the technology [71], [72].

2.1.3 Selling and Sharing of Data

Children's data generated by AI may be shared with or sold to other individuals, institutions, or businesses – including data brokers – often without prioritization of children's interests [51]. With the emergence of the data economy, information is now one of the most valuable commodities for many industries [73]. Children represent valuable sources of data in this context. Children influence the consumer decisions of their families and may also be significant consumers themselves, both today and in the future as adults [61]. As such, the combination, sharing, and onselling of children's data are occurring at an intensive rate, with the increasing spread of AI-enabled products and services amplifying opportunities for their data to be exploited for profit [74].

This selling and sharing of children's data mean that information may be used in both commercial and institutional contexts unrelated to the original intent, with AI potentially yielding new purposes for use [65]. In addition to contravening privacy norms generally, the use of children's data in different contexts by different actors could have consequential impacts on their lives [69]. For instance, children's data from online platforms could potentially be shared with unexpected parties, including admissions offices, employers, insurers, or even the police, with life-changing implications.

AI technologies may also enable unauthorized actors to access children's information due to insecure data storage or devices [41]. Breaches of large datasets are common occurrences for IoT devices that children use like Internet-connected smart toys. For example, one toy company had a data breach in 2015 that exposed the information of 500,000 Canadian children and parents [75]. Hackers may also target these toys directly, in addition to other AI-enabled devices like smart speakers and doorbells, since physical devices may allow the direct surveillance of children [76].

2.1.4 Lifespan of Data

Research interviewees noted that the data that AI collects may have a long lifespan; children's information may persist as a "data shadow" that follows them across the entirety of their lives. The long-term retention of children's data is in tension with the fact that they may change their privacy preferences as they grow older or have different preferences than the parents who consented on their behalf [51]. It also undermines the efficacy of AI systems as the use of outdated data can lead to incorrect analyses and problematic outcomes [69].

The long shadow of childhood data also means that children's information may be used in AI applications that impact their future adult lives, undermining their ability to make mistakes and freely explore their world during childhood [77]. Advocates are concerned that data gathered during childhood could one day influence adult opportunities and access to services such as health insurance and post-secondary education [70].

2.2 Function Risks

Risks to children's privacy from AI systems extend beyond data exploitation. How data are used in multi-layered processing models may lead to certain tasks or functions that infringe on children's privacy [1], [78]. Namely, AI can be used to conduct data inference and re-identification, surveillance, profiling, and decision-making at rapid speeds and scales. These functions frequently overlap and coincide with one another. While the privacy risks posed by the use of AI in these tasks are not necessarily unique to children, they may have deeper, longer-lasting, and more consequential impacts for this demographic.

2.2.1 Data Inference and Re-Identification Functions

Two core strategies commonly used to protect children's privacy include "anonymizing" or delinking datasets with potentially sensitive information, and intentionally not collecting or sharing personally identifiable information. However, the growth of AI poses new, destabilizing challenges to both these strategies.

First, by analyzing large amounts of data and identifying links, some applications of AI can be used to re-identify previously anonymized data [79]. As an illustration, researchers did a study where they inputted partially aggregated "health activity data" generated from health wearables into a machine-learning algorithm to find out if re-identifying participants was possible [80]. Their algorithm was able to correctly re-identify over 95% of adults and over 85% of children who participated in the survey. Second, AI systems can also be used to infer or "generate" sensitive data that have not been disclosed by combining and making connections between seemingly unrelated and innocuous pieces of non-personal information [81]. For instance, AI can use a child's behavioural data from online platforms to infer sensitive information like age, race, and location without asking for that information.

2.2.2 Surveillance Functions

AI has enabled the proliferation of always-on and real-time mass surveillance by both private and public actors [32]. Through these technologies, children can be identified and monitored as they navigate both digital and physical spaces. For instance, some schools use facial recognition to track student movement across campus, while others use online platforms that monitor student conduct online [37], [82]. Children may also be incidentally captured by AI-enabled surveillance tools designed for the general public. In 2019, the Amazon-owned smart doorbell company Ring published data that showed their doorbells had rung over 15 million times on Halloween, displaying Ring-captured footage of children approaching houses [83]. While the publication blurred children's faces, the case exemplifies how many children may be under constant surveillance by AI-enabled technologies, even when exploring their neighbourhoods.

This pervasive surveillance by external forces may have a particular impact on children and their development. Knowledge of constant surveillance may transform children's expectations of appropriate anonymity and privacy, influence their identity construction, and undermine their development of trusting relationships [32], [84]. It may also create "chilling effects" on

"Constant surveillance may transform children's expectations of appropriate anonymity and privacy, influence their identity construction, and undermine their development of trusting relationships."

behaviour and limit their ability and willingness to take risks, express themselves, search for sensitive information, and access helplines [23], [85].

2.2.3 Profiling Functions

AI can also profile children by using their data in algorithms to evaluate aspects of their identities and lives, including their personality, preferences, and performance [86]. AI systems can categorize, assess, and rank children in personal and often opaque ways that are challenging to contest [87]. These AI-generated profiles can also become data points themselves, used in further analysis by AI or to make critical decisions about children and their opportunities.

Available evidence demonstrates that AI profiling is often inaccurate or biased, facilitating discrimination and unfairness [86]. Yet it is already used widely in fields such as advertising and is expected to have a greater impact on children by virtue of the heightened availability of their data [70]. Predictive profiling is also particularly concerning in the case of children since it may influence or undermine a child's capacity to change, grow, and transform in the future.

2.2.4 Decision-Making Functions

AI can make or inform predictions and critical decisions about children and their environments, often on the basis of system-generated profiles [87]. Automated and semi-automated decision-making are already common in children's lives, generally in "low-stakes" applications like content moderation. However, AI prediction and decision-making are increasingly being deployed in "high-stakes" applications like child protective services, university admissions, and employment [70]. As AI grows in both prevalence and capability, AI-enabled decisions could replace human decision-making in instances that meaningfully influence the trajectory of children's lives [41]. But the opacity or "black box" of AI makes these algorithmic decisions less explainable, less transparent, and less easy to meaningfully contest [36].

2.3 Oversight Risks

Many experts and advocates agree on ideals that should inform AI governance and oversight, even as opinions on implementation diverge. Consistent themes include the importance of **fairness**, **transparency and explainability**, and **accountability** [88], [89]. Each of these relate to children's privacy because they support responsible oversight of how AI uses children's information in functions that impact their lives.

2.3.1 Fairness

In principle, AI should be deployed in ways that are accurate and fair, promoting inclusive access and equitable outcomes without discrimination based on age, race, gender, disability, location, or socio-economic status [6]. However, as a product of both human design and human-generated data, AI frequently reproduces or even deepens existing human

biases [86], [90]. As such, AI systems have consistently made errors and demonstrated embedded biases, with potentially discriminatory and unfair impacts that may perpetuate and exacerbate existing inequalities [65].

Organizations like the Algorithmic Justice League have brought attention to the many cases where AI perpetuates and amplifies racism, sexism, ableism, and other forms of discrimination for adults and children alike [91]. For example, a study of 189 facial recognition algorithms found that those systems falsely identified Black and Asian faces 10 to 100 times more frequently than Caucasian faces [92]. Researchers have also uncovered algorithmic bias in health care, with AI incorrectly assessing Black patients as being less at risk than they actually were [93].

This potential for unfairness and discrimination from AI relates to children's privacy because it includes the use of their information in ways that are against their best interest [94]. However, stricter limitations on children's data may be in tension with efforts to dismantle algorithmic bias because bias can come from a lack of appropriately big and inclusive data sets to train AI systems. AI can be less accurate or fair in generating child-appropriate decisions when it has not learned from child-generated data. This may be especially true for children who belong to groups already underrepresented in datasets, including racialized children, children in poverty, and gender non-conforming children [6].

2.3.2 Transparency and Explainability

In principle, to the greatest extent possible, individuals should be informed when AI is being used in ways that may impact them. People should also be provided with information on why AI is being used, what information it is using, and how outcomes are generated [95]–[97]. However, the sophisticated mechanisms of AI are often opaque – like a black box – with the relation between inputs and outcomes difficult to discern and understand, even for experts [32]. Generally, the more sophisticated and powerful an AI system is, the more opaque it is to human review or analysis.

The potential lack of transparency of AI systems in children's lives has implications for their privacy because it makes it difficult for them to determine if their information has been used fairly and accurately, to challenge or contest any automated decisions, and to gain redress for harms [81]. It also adds an additional layer of complexity to the thorny issue of children's consent to data collection and AI use. Asking a parent or child to share information without being able to say how that information will be used by AI means the present notice-and-consent regime is not able to meaningfully support children's privacy.

2.3.3 Accountability

In principle, those who design, approve, deploy, or profit from AI systems should be identifiable and held accountable for any negative impacts or harms that flow from those systems whether intended or not [96]. However, there are few clearly defined guidelines for responsible AI use, let alone sanctions for non-compliance, nor are there efficient processes to challenge outcomes and seek redress [76]. This is particularly problematic where children are concerned as they often have less capacity and fewer resources to respond to any privacy violations or harms [17], [51].

Experts and children's advocates interviewed for this project sounded the alarm about the perverse incentives that allow the commodification of children's private information to be a successful and growing industry. A regulatory environment with few carrots and almost no sticks means that there are few accountability requirements competing with these profit incentives.

3 Recommendations to Promote Children's Privacy

While reforms to privacy legislation in Canada are being considered to address novel risks created by AI, the needs of children are missing from the policy conversation. Instead, policy designed for everyone has largely meant policy designed for adults-by-default. There is an urgent need to change course and

develop a child-specific approach to privacy promotion that considers the deep and distinct impact of AI on children's lives.

A well-designed policy response depends on a range of policy tools that include legislation, regulatory guidance, standards, technological innovations, and education initiatives [98]. The development of these responses should also include cross-sector stakeholders from AI developers to children's rights advocates [6].

Any policy development that aims to promote children's privacy in the context of AI must be grounded in their perspectives, by applying these cross-cutting actions:

- **Consider children as a distinct and vulnerable population:** Children need to be recognized as a distinct and vulnerable class of individuals in any legislation, regulation, or other policy intervention in recognition of their specific privacy rights, needs, and circumstances. Without this recognition, tools will be designed for the majority (adults) and protections of children's privacy will be insufficient, ineffective, or missing [17].
- **Involve children in privacy and AI policy development:** Children have a fundamental right to participate in decisions on issues that affect their lives and the world they will inherit, with their input given due weight [6]. Today's children are also the only people who have experienced the realities of growing up with AI [99].

In addition to these cross-cutting factors, different types of interventions aimed at preserving children's privacy are needed across the lifecycle of AI – before deployment, during adoption, and after use, as depicted in Figure 4.

3.1 Before Deployment: Design and Development of AI Systems

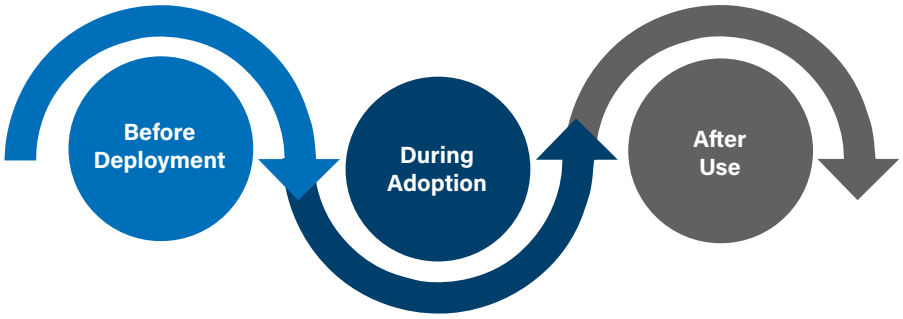
Before AI technologies ever reach the market, children's privacy rights need to take precedence in their design. The responsibility for the protection of privacy rights and needs should lie with organizations creating and deploying the technology, rather than children and their caregivers.

3.1.1 Mandate and Operationalize Children's Privacy by Design

Children's privacy should be embedded into the priorities of organizations and their development or procurement of AI technologies. Following a design approach, organizations should be required to create their technologies with children's privacy in mind, with consideration given to data collection and processing, as well as the functionalities and applications of AI systems from initial ideation and throughout the development process [6]. This will help generate AI systems that function to promote children's privacy from the start, rather than attempting to solve privacy challenges after the fact. Notable frameworks that have been developed to operationalize this design philosophy include Privacy by Design and Human Rights by Design [100], [101].

Other jurisdictions mandate similar "by design" practices, such as in Article 25 of the *General Data Protection Regulation* (GDPR), which provides for "Data protection by design and by default" [102].

Figure 4: Recommendations across the life cycle of AI



Canadian institutions such as the Office of the Privacy Commissioner of Canada (OPC) have also proposed a "by design" approach and could provide further guidance on actions to implement it for children, setting out rules for how organizations should design systems and processes in respect to their distinct privacy rights, needs, and circumstances [97].

The UK's Information Commissioner's Office's (ICO) *Children's Code* (formally called the Age Appropriate Design Code) provides a useful statutory code of practice that Canada could emulate [103], [104]. The *Children's Code* outlines 15 flexible standards that help to ensure practices that promote children's privacy and best interests are in place by default [105]. These standards include minimizing data collection and retention, switching off geolocation settings, and avoiding nudge techniques. The *Children's Code* applies not only to online products or services directly targeted at children under 18 but also to technologies that are likely to be accessed by them [105].

In addition to overarching guidance from oversight institutions or regulatory bodies, Standards Development Organizations (SDOs) may serve to support these rules, specifying how to operationalize children's privacy by design [106], [107]. This could include the development of standards targeted at specific sectors, such as education systems, and for specific products or services, such as IoT devices [108]. Ongoing standards development related to children's privacy and AI includes work by the Institute of Electrical and Electronics Engineers Standards Association (IEEE SA) to develop a family of standards for AI and a suite of standards for age-appropriate digital services based on the 5Rights Framework [109], [110]. The latter focuses on presenting information in an age-appropriate way, upholding children's rights, offering fair terms for children, recognizing childhood, and putting the child ahead of commercial interests and platform status.

3.1.2 Require Children's Privacy Impact Assessments

Independent privacy impact assessments can offer due diligence before procurement and deployment and on an ongoing basis [6], [79]. These assessments test algorithms and data sets, assess legal and regulatory compliance, and evaluate implications for children's privacy rights [51]. Effective impact assessment processes involve children in the evaluation [68].

The results should be transparent, easy to understand, and accessible to children and their caregivers. There is a potential role for standards in defining what the assessments should look like such as rules governing layout, content, and accessibility [102].

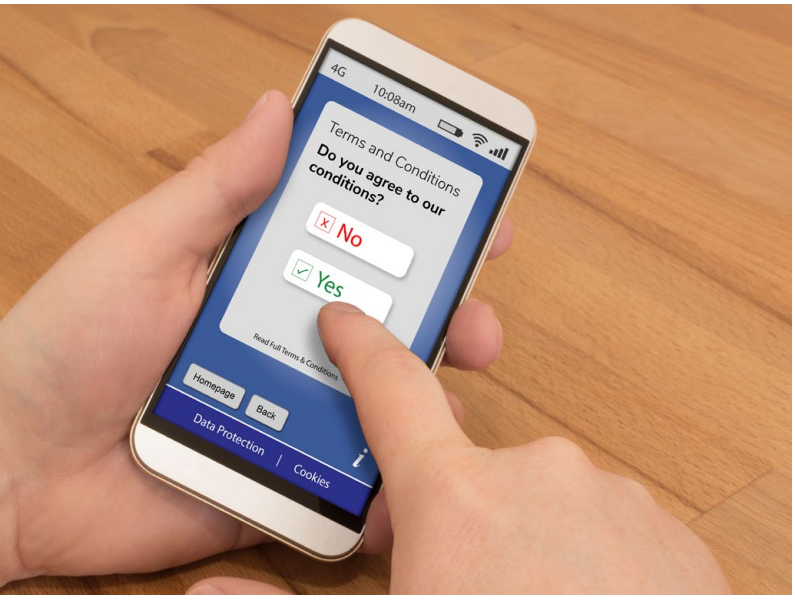
Children's privacy impact assessments could be made mandatory. Article 35 of the GDPR creates an obligation for organizations to conduct a data protection impact assessment if processing is likely to lead to high risk for the rights and freedoms of persons [12]. Under this condition, online services directly targeted at children and the use of children's personal data for marketing, profiling, and other automated decision-making are considered high risk [105], [111]. Alternatively, guidelines for children's privacy impact assessments and independent verification processes could be created through trusted industry actors or SDOs.

3.2 During Adoption: User Privacy and Choice

Children and their caregivers need to be equipped with the right tools to manage privacy when using AI technologies. There is no single intervention or "silver bullet" when it comes to successfully moderating the relationship between children and AI systems, especially when it comes to promoting informed consent. Actions must be taken by a variety of stakeholders – governments, private industry, children's educators, regulatory leaders – to ensure children have distinct options, age-appropriate understanding, and meaningful choice as data subjects in a connected world.

3.2.1 Develop Educational Resources for Children, Teachers, and Parents

Education programs that support AI literacy for children and their caregivers are essential tools for promoting children's privacy. Introducing these concepts may be a challenge; there is already so much ground to cover in media education for children,



"The current language of most privacy agreements is not helpful for children, or even adults."

and digital privacy is just one component. However, to support children's privacy, it is necessary to go beyond e-safety concepts of "stranger danger" and deliver age-appropriate education that builds children's understanding of privacy rights, commercial interests, and governance [112]. To do this, it is important for children to engage with the more abstract privacy considerations associated with data and its use by AI, including profiling, decision-making, and inference [6].

Building age-appropriate education on privacy, data, and AI into school curriculum is an effective way to ensure children from all backgrounds and levels of digital proficiency gain a functional understanding of AI and their privacy rights [6], [113]. Organizations like MediaSmarts and Kids Code Jeunesse are bringing AI-specific education to classrooms across Canada, including resources for teachers and parents [114], [115].

3.2.2 Require Child-Friendly Notices and Terms of Service

Despite challenges to meaningful consent in the digital era, especially for children, it remains central to personal autonomy [9], [116]. Acknowledging the flaws that characterize most notice-and-consent regimes does not mean that decision-makers should abandon the pursuit of *more* informed consent frameworks or that industry actors should not be accountable for enabling users to make more informed choices. Efforts should be made to develop standards for accessible terms of service that give explicit notification about the use of AI and data processing.

The current language of most privacy agreements is not helpful for children, or even adults. Research shows that a large share of privacy agreements require a postsecondary-level reading ability or higher to understand; a 2019 study in *The New York Times* reviewed 150 privacy policies and called most "an incomprehensible disaster" [117]. Promising research has been done with both children and adults on methods to make these agreements more accessible and useful to users. These strategies include using plain language, accompanying text with videos and graphics – CSA's report *Rethinking Privacy Agreements* suggests pictograms as a form of graphic – and providing interactive components like multiple checkboxes [66], [118].

Child-friendly terms of service agreements should be incorporated into all AI-enabled products and services that routinely collect and use children's information. This should occur even when technologies are not specifically intended for children and when children are directed to ask a parent to read and consent on their behalf. Both children and parents should be notified upfront when AI is operating and be provided information on how their data are being used, retained, and shared. Ideally, age-appropriate privacy agreements would also support privacy personalization with more dynamic and granular options for consent [66].

3.2.3 Encourage Certification and Consumer Labelling

Certification of AI-enabled products and services that adhere to standards and best practices for promoting children's privacy could be another tool to help children and their caregivers make more informed choices [119]. Action is already underway to develop such conformity assessment programs for the general public, and these could be supplemented or adapted to be child-specific. For instance, the IEEE SA is developing certification criteria for both the advancement of transparency and accountability, and the reduction of algorithmic bias in Autonomous and Intelligent Systems (AIS) [120].

Introducing standardized and easy-to-understand labelling for AI-enabled products and services is another way to empower choice. Privacy "nutrition labels" can provide prospective users with key indicators of privacy and information use in a format already familiar to consumers [121], [122]. For instance, in 2020, Apple began requiring developers for all apps in the App Store to have data privacy labels that indicate the kind of information that will be shared with the app, including things like location, financial information, or third-party disclosures [123], [124].

Systems like the one being introduced by Apple are a promising development but a more standardized approach might be needed to provide a consistent labelling regime useful to consumers [102]. Such standardized labels are being explored for AI technologies. For instance, researchers at Carnegie Mellon University have developed a prototype for a "security and privacy label" for IoT technologies [125]. Similarly, a Canadian multi-stakeholder group exploring best practices for IoT technology recommended labelling and "trustmarks" for IoT devices aligned with international-level standards [126]. Implementing this kind of privacy labelling or certification across all available AI technologies would be a large undertaking, but a good place to start would be products and services specifically geared for children.

3.2.4 Provide Dynamic and Granular Consent Options

To be more effective, consent frameworks should go beyond making a child or parent more aware of what they consent to when they click "I Agree". Movement away from the fixed binary of "wholesale consent" or "no consent" to more dynamic and granular consent options would help people be empowered to manage their privacy choices. This is especially true for children, as their agency will increase as they grow and their desires around privacy options may change over time.

There is a trend in privacy legislation towards providing more variable consent options and choice for data subjects in the face of digital technologies and particularly automated decision-making. But enforcement and implementation of these legislative principles are still in early stages. Such protections and rights include:

- **A right to object to automated decision-making:** This right provides individuals with the right to choose not to be subject to solely automated decision-making and profiling and the right to request human intervention [15].
- **A right to explanation:** This right provides individuals with the right to an explanation of the reasoning and elements behind automated processing, and any consequences for their rights and interests [15], [97].
- **A right to be forgotten (RTBF):** This right provides individuals with the right to compel another party to withdraw, remove, and erase their personal data [127], [128]. The case for the RTBF is especially urgent in the case of children because of the understanding that choices made by children as they learn, grow, and develop should not have enduring or permanent consequences [129].

In addition to legislative compliance, major online platforms like Google, Facebook, and Snapchat have enhanced options for customized privacy settings, but a user must proactively select to review the options and adjust the settings themselves [129]. Simplified privacy dashboards or prompts to review or adjust one's individual user settings are some ways to proactively support meaningful, ongoing consent for children.

3.3 After Use: Oversight and Accountability

Oversight and accountability interventions are needed to monitor AI systems, adjudicate contested outcomes, and hold actors responsible for violations to children's privacy and any associated harms [6]. Organizations need to consistently monitor their AI systems to prevent and resolve any issues. Children also need independent institutions that will audit organizations on their behalf for violations, support them in asserting their privacy rights, and provide pathways for redress if any harms occur [14].

3.3.1 Mandate Organizational Oversight Mechanisms

Within organizations developing and deploying AI, processes need to be implemented to provide oversight and responsibility for children's privacy. At the level of AI systems, this could include human intervention to review processes and results and disclose any negative implications on children's privacy [98]. At the organizational level, entities that implement AI systems could also be required to have internal Privacy Officers who would provide identifiable leadership and accountability. These actors would be responsible for their organization's compliance with legislation and review of processes for potential harms to children's privacy, and would act as a touchpoint for information and potential privacy complaints [102], [130].

3.3.2 Fund Independent Oversight Institutions

Independent oversight institutions are needed to monitor the application of AI systems by organizations and hold institutions accountable for any infringement on children's privacy rights that may occur during use. This could be achieved by expanding the scope, mandate, and independence of existing organizations. Their role may include audits, reporting mechanisms, and complaint mechanisms [85], [94], [130].

Given children's ongoing development and heightened vulnerability, they may face particular difficulties in gaining access to justice for violations of their privacy [85]. As such, oversight institutions should have information, complaint, and reporting mechanisms that are prompt, widely-known, and child-friendly, with specific supports for children and their advocates throughout any investigative or judicial process on violations of privacy [85]. To do so meaningfully, these institutions will also require sufficient funding and enforcement powers in order to allocate impactful consequences for violations of children's privacy from AI systems [6], [97]. Oversight actors need the power to compel records, raw data, and witnesses for investigations; issue binding orders; and impose penalties, fines, or sanctions [14], [131].

If Canada's Bill C-11 is passed, the OPC will be given order-making powers and a proposed Personal Information and Data Protection Tribunal will adjudicate penalties [132]. This is an important step towards ensuring accountability for privacy violations and redress for harms from AI systems. But further child-specific mechanisms that account for the fact that children are likely not to have the capacity to make a claim independently are needed. This could include the creation of a Children's Privacy Advocate role within the OPC that has a specific mandate to monitor for violations of children's privacy and bring collective complaints on their behalf.

3.3.3 Introduce Strict Penalties for Privacy Violations

In order to create accountability and deter non-compliance, consequences for violations need to substantially exceed the profit or other benefits that come from infringing on children's privacy rights [97]. These remedial tools should be particularly strict in the case of children, given their relative vulnerability and the potential for long-term harm from violations of their privacy [85]. In California, under the *California Privacy Rights Act,* fines for privacy violations are higher if a business has knowledge that affected individuals included children under 16 years old [133]. This type of enhanced consequence may distinctly discourage violations of children's privacy and encourage the active promotion of their privacy among organizations.

Conclusion

AI is fundamentally changing the world children live in, bringing both opportunities and challenges. Increasingly, children's everyday spaces and activities are embedded with this technology – from play, to learning, to health care – expanding the information that can be gleaned about them, transforming how they can be identified and tracked, and influencing critical decisions about their lives.

While the privacy risks of AI are often less apparent than privacy intrusions of the analogue era, they magnify existing issues and create new challenges. Without proper stewardship and action, AI risks may pose substantial and negative consequences for children, both today and in the future. Promoting children's privacy in the age of AI is therefore critical to ensuring their healthy development, well-being, and other rights.

AI is an emerging technology, leaving many uncertainties. It is certain, however, that children are current users of AI systems and stand to inherit a world ever more saturated by these technologies. Yet AI product and service design, and corresponding policy responses, largely do not consider the specific privacy rights, needs, and circumstances of children. Children's evolving capacities and best interests will not be respected under these circumstances.

Given the rapid pace of technological change and potential for harm, AI and privacy conversations and policy development need to focus on children now. This will require different types of interventions and the active participation of many stakeholders across industry, government, and civil society. But most importantly, it will necessitate inclusion of children's own voices, ideas, and perspectives. Some steps could include industry standards that centre children's privacy by design, child-friendly terms of services that allow them to make more informed decisions, and stronger penalties for privacy violations that deter non-compliance and offer children avenues for redress.

Society's impulse to empower and protect children is a strong force that has proven downstream effects for adults. It helps us prioritize well-being in the face of change and new technologies. A targeted effort to make the world of AI better for children contains the possibility of a world of AI that is better for everyone.

A full summary of these recommendations can be found in Table 1.

Table 1: Summary of recommendations

Cross-cutting actions		
Consider children as a distinct and vulnerable population		
Involve children in privacy and AI policy development		
Interventions across the life cycle of AI		
Before deployment	**During adoption**	**After use**
Mandate and operationalize children's privacy by design	Develop educational resources for children, teachers, and parents	Mandate organizational oversight mechanisms
Require children's privacy impact assessments	Require child-friendly notices and terms of service	Fund independent oversight institutions
	Encourage certification and consumer labelling	Introduce strict penalties for privacy violations
	Provide dynamic and granular consent options	

Acknowledgements

The authors would like to thank workshop participants and research interviewees for sharing their experience and expertise. The authors are also grateful to all of the members of the project advisory panel for their input and advice.

References

[1] Future of Privacy Forum, "The privacy expert's guide to artificial intelligence and machine learning," FPF, Oct. 2018. [Online]. Available: https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdf

[2] Organisation for Economic Co-operation and Development, *Artificial Intelligence in Society,* Paris, France: OECD Publishing, 2019.

[3] Office of the Privacy Commissioner of Canada, "The Internet of Things: An introduction to privacy issues with a focus on the retail and home environments,"OPC, Feb. 2016. [Online]. Available: https://www.priv.gc.ca/media/1808/iot_201602_e.pdf

[4] Organisation for Economic Co-operation and Development, *An Introduction to Online Platforms and Their Role in the Digital Transformation.* Paris, France: OECD Publishing, 2019.

[5] UN General Assembly, (*Resolution 44/25, Convention on the Rights of the Child,* Nov. 20, 1989. [Online]. Available: https://www.ohchr.org/Documents/ProfessionalInterest/crc.pdf

[6] UNICEF Office of Global Insight and Policy, *Policy Guidance on AI for Children* (Draft 1.0), Sep. 2020. [Online]. Available: https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf

[7] R. Vinuesa et al., "The role of artificial intelligence in achieving the Sustainable Development Goals," *Nat. Commun.,* vol. 11, no. 1, pp. 1–10, Jan. 2020, doi: 10.1038/s41467-019-14108-y

[8] House of Commons of Canada, 43rd Parliament, 2nd session, Bill C-11, Digital Charter Implementation Act, Nov. 17, 2020. [Online]. Available: https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading

[9] N. Zon and A. Lipsey, *Children's Safety and Privacy in the Digital Age,* CSA Group, Toronto, ON, CAN, May 2020. [Online]. Available: https://www.csagroup.org/article/research/childrens-safety-and-privacy-in-the-digital-age/

[10] M. Penagos, S. Kassir, and S. Vosloo, "National AI strategies and children: Reviewing the landscape and identifying windows of opporunity," UNICEF Office of Global Insight and Policy, New York, NY, USA, Sep. 2020. [Online]. Available: https://www.unicef.org/globalinsight/media/1156/file

[11] I. Cofone, "Policy proposals for PIPEDA reform to address artificial intelligence," OPC, Nov. 12, 2020. [Online]. Available: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pol-ai_202011/

[12] European Parliament and the Council of Europe, *Regulation (EU) 2016/679, General Data Protection Regulation,* Apr. 27, 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[13] Office of the Privacy Commissioner of Ontario, "Canada's access to information and privacy guardians urge governments to modernize legislation to better protect Canadians," OPC, Nov. 6, 2019. [Online]. Available: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/nr-c_191106/

[14] Office of the Privacy Comissioner of Ontario, "Effective privacy and access to information legislation in a data driven society: Resolution of the Federal, Provincial and Territorial Information and Privacy Commissioners," OPC, Oct. 1-2, 2019. [Online]. Available: https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_191001/

[15] Office of the Privacy Commissioner of Canada, "Consultation on the OPC's proposals for ensuring appropriate regulation of artificial intelligence," OPC, Jan. 28, 2020. [Online]. Available: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pos_ai_202001/

[16] Department of Justice, "Respect, accountability, adaptability: A discussion paper on the modernization of the *Privacy Act*," Government of Canada, Nov. 17, 2020. [Online]. Available: https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/raa-rar.html

[17] S. Livingstone, J. Carr, and J. Byrne, "One in three: Internet governance and children's rights," *Innocenti Discussion Papers,* no. 2016-01, Jan. 2016. [Online]. Available: https://www.unicef-irc.org/publications/795-one-in-three-internet-governance-and-childrens-rights.html

[18] M. Penagos, "What do national AI strategies say about children? Reviewing the policy landscape and identifying windows of opportunity," UNICEF Office of Global Insight & Policy, Sep. 8, 2020. [Online]. Available: https://www.unicef.org/globalinsight/stories/what-do-national-ai-strategies-say-about-children

[19] UNICEF Office of Innovation, "Generation AI." [Online]. Available: https://www.unicef.org/innovation/GenerationAI (accessed Nov. 14, 2020).

[20] Beijing Academy of Artificial Intelligence, "Artificial intelligence for children: Beijing principles," Sept. 14, 2020. [Online]. Available: https://www.baai.ac.cn/ai-for-children.html

[21] S. Perez, "COVID-19 quarantine boosts smart speaker usage among U.S. adults, particularly younger users," *TechCrunch,* Apr. 30, 2020. [Online]. Available: https://techcrunch.com/2020/04/30/covid-19-quarantine-boosts-smart-speaker-usage-among-u-s-adults-particularly-younger-users/

[22] N. Perlroth, "Verifying ages online is a daunting task, even for experts," *The New York Times,* Jun. 17, 2012. [Online]. Available: https://www.nytimes.com/2012/06/18/technology/verifying-ages-online-is-a-daunting-task-even-for-experts.html

[23] M. Cardinal-Bradette et al., "Executive summary: Artificial Intelligence and children's rights," UNICEF Innovation and UC Berkeley Human Rights Center, May 2019. [Online]. Available: https://www.unicef.org/innovation/reports/memoAIchildrights

[24] Future of Privacy Forum, "Kids and the connected home: Privacy in the age of connected dolls, talking dinosaurs, and battling robots," FPF, Dec. 2016. [Online]. Available: https://fpf.org/wp-content/uploads/2016/11/Kids-The-Connected-Home-Privacy-in-the-Age-of-Connected-Dolls-Talking-Dinosaurs-and-Battling-Robots.pdf

[25] K. L. Smith and L. R. Shade, "Children's digital playgrounds as data assemblages: Problematics of privacy, personalization, and promotional culture," *Big Data Soc.,* pp. 1–12, Oct. 2018, doi: 10.1177/2053951718805214.

[26] G. Chu, N. Apthorpe, and N. Feamster, "Security and privacy analyses of Internet of Things children's toys," *IEEE Internet Things J.,* vol. 6, no. 1, pp. 978–985, Aug. 2019, doi: 10.1109/JIOT.2018.2866423.

[27] P. C. K. Hung, F. Iqbal, S.-C. Huang, M. Melaisi, and K. Pang, "A glance of child's play privacy in smart toys," in *Cloud Computing and Security,* X. Sun, A. Liu, and E. Bertino, Eds., Lecture Notes in Computer Science, vol. 10040, Cham, Switzerland: ICCCS, 2016, pp. 217–231, doi: 10.1007/978-3-319-48674-1_20.

[28] V. Barassi, "'Home life data' and children's privacy," Child Data Citizen, Sep. 18, 2018. [Online]. Available: http://childdatacitizen.com/cdc/wp-content/uploads/2018/09/'HOME-LIFE-DATA'-AND-CHILDREN'S-PRIVACY-1.pdf

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

[30] S. Gibbs, "Hackers can hijack Wi-Fi Hello Barbie to spy on your children," *The Guardian,* Nov. 26, 2015. [Online]. Available: https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children

[31] E. McReynolds, S. Hubbard, T. Lau, A. Saraf, M. Cakmak, and F. Roesner, "Toys that listen: A study of parents, children, and internet-connected toys," in *Conf. on Human Factors in Comput. Syst. – Proc.,* 2017, pp. 5197–5207, doi: 10.1145/3025453.3025735.

[32] M. Cardinal-Bradette et al., "Memorandum on artificial intelligence and child rights," UC Berkeley Human Rights Center, Berkeley, CA, USA, Apr. 2019. [Online]. Available: https://www.unicef.org/innovation/reports/memoAIchildrights

[33] L. Plunkett and U. Gasser, "Student privacy and Ed Tech (K-12)," *Berkman Klein Cent. Internet Soc. Publ. Ser.,* pp. 1–11, Sep. 2016. [Online]. Available: http://nrs.harvard.edu/urn-3:HUL.InstRepos:28552586

[34] L. Plunkett, U. Gasser, and S. Cortesi, "Student privacy and the law in the Internet Age," in *The Oxford Handbook of U.S. Education Law,* K. L. Bowman, Ed. Oxford, UK: Oxford University Press, 2019, pp. 1–24.

[35] M. Bulger, "Personalized learning: The conversations we're not having," Data & Soceity Research Institute, Jul. 22, 2016. [Online]. Available: https://datasociety.net/pubs/ecl/PersonalizedLearning_primer_2016.pdf

[36] E. Zeide, "Robot teaching, pedagogy, and policy," in *The Oxford Handbook of Ethics of AI,* M. D. Dubber, F. Pasquale, and S. Das, Eds., Oxford, UK: Oxford University Press, 2020.

[37] S. Stolzoff, "Schools are using AI to track their students," *Quartz,* Aug. 19, 2018. [Online]. Available: https://qz.com/1318758/schools-are-using-ai-to-track-what-students-write-on-their-computers/

[38] S. Swauger, "Software that monitors students during tests perpetuates inequality and violates their privacy," *MIT Technology Review,* Aug. 7, 2020. [Online]. Available: https://qz.com/1318758/schools-are-using-ai-to-track-what-students-write-on-their-computers/

[39] T. Evgeniou, D. R. Hardoon, and A. Ovchinnikov, "What happens when AI is used to set grades?" *Harvard Business Review,* Aug. 13, 2020. [Online]. Available: https://hbr.org/2020/08/what-happens-when-ai-is-used-to-set-grades

[40] H. J. Han, "An algorithm shouldn't decide a student's future," *Human Rights Watch,* Aug. 13, 2020. [Online]. Available: https://www.hrw.org/news/2020/08/13/algorithm-shouldnt-decide-students-future

[41] A. Hasse, S. Cortesi, A. Lombana-Bermudez, and U. Gasser, "Youth and Artificial Intelligence: Where we stand," Youth and Media, Berkman Klein Center for Internet & Society, Cambridge, MA, USA, May, 2019. [Online]. Available: https://cyber.harvard.edu/publication/2019/youth-and-artificial-intelligence/where-we-stand

[42] D. Lupton, "Data assemblages, sentient schools and digitised health and physical education (response to Gard)," *Sport. Educ. Soc.,* vol. 20, no. 1, pp. 122–132, Oct. 2014, doi: 10.1080/13573322.2014.962496.

[43] S. K. Glaberson, "Coding over the cracks: Predictive analytics and child protection," *Fordham Urban Law J.,* vol. 46, no. 2, p. 363, Apr. 2019. [Online]. Available: https://ir.lawnet.fordham.edu/ulj/vol46/iss2/3

[44] K. Robertson, C. Khoo, and Y. Song, "To surveil and predict: A human rights analysis of algorithmic policing in Canada," Citizen Lab, Toronto, ON, CAN, Sep. 2020. [Online]. Available: https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf

[45] S. O'Flynn, "Protecting children's data privacy in the smart city," *The Conversation,* May 19, 2019. [Online]. Available: https://theconversation.com/protecting-childrens-data-privacy-in-the-smart-city-113319

[46] Office of the Privacy Commissioner of Canada, "News release: Cadillac Fairview collected 5 million shoppers' images," *OPC,* Oct. 29, 2020. [Online] Available: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_201029/

[47] K. Allen, "Cadillac Fairview broke privacy laws by using facial recognition technology at malls, investigators conclude," *Toronto Star,* Oct. 29, 2020. [Online]. Available: https://www.thestar.com/news/gta/2020/10/29/cadillac-fairview-broke-privacy-laws-by-using-facial-recognition-technology-at-malls-investigators-conclude.html

[48] Centre for Public Impact, "The Allegheny Family Screening Tool: Predictive risk modeling in child welfare in Allegheny County" Centre for Public Impact, Washington, DC, USA, Oct. 2018. [Online]. Available: https://www.alleghenycounty.us/Human-Services/News-Events/Accomplishments/Allegheny-Family-Screening-Tool.aspx

[49] 5Rights Foundation, "The 5Rights Framework." [Online]. Available: https://5rightsfoundation.com/about-us/the-5-rights/ (accessed Nov. 27, 2020).

[50] G. Lansdown, "The Evolving Capacities of the Child," UNICEF Innocenti Research Centre, Florence, Italy, Nov. 2005. [Online]. Available: https://www.unicef-irc.org/publications/pdf/evolving-eng.pdf

[51] UNICEF, "Children's rights and busines in a digital world: Privacy, protection of personal information and reputation rights," *Discussion Paper Series: Children's Rights and Business in a Digital World,* Mar. 2017. [Online]. Available: https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf

[52] J. Peter and P. M. Valkenburg, "Adolescents' online privacy: Toward a developmental perspective," in *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web,* S. Trepte and L. Reinecke, Eds., Berlin, Germany: Springer Publishing, 2011, pp. 221–234, doi: 10.1007/978-3-642-21521-6_16.

[53] Access Now, "Human rights in the age of artificial intelligence," Access Now, New York, NY, USA, Nov. 2018. [Online]. Available: https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf

[54] S. Livingstone, E. Lievens, S. McLaughlin, D. Miles, B. O'Neill, and V. Verdoodt, "Policy guidance on empowering, protecting and supporting children in the digital environment," Council of Europe, Strasbourg, France, Nov. 2018. [Online]. Available: https://edoc.coe.int/en/children-and-the-internet/8011-policy-guidance-on-empowering-protecting-and-supporting-children-in-the-digital-environment.html

[55] S. Livingstone, M. Stoilova, and R. Nandagiri, "Children's data and privacy online: Growing up in a digital age," London School of Economics and Political Science, London, UK, Dec. 2018. [Online]. Available: https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf

[56] B. Shmueli and A. Blecher-Prigat, "Privacy for Children," *Columbia Human Rights Law Rev.,* vol. 42, pp. 759–795, Jan. 2011. [Online]. Available: https://ssrn.com/abstract=1746540

[57] W. Leung, "How will AI technologies affect child development?" *The Globe and Mail,* Jul. 31, 2018. [Online]. Available: https://www.theglobeandmail.com/life/article-how-will-ai-technologies-affect-child-development/

[58] B. B. Kidron and A. Rudkin, "Digital childhood: Addressing childhood development milestones in the digital environment," 5Rights Foundation, London, UK, Dec. 2017. [Online]. Available: https://5rightsfoundation.com/static/Digital_Childhood_report_-_EMBARGOED.pdf

[59] Information Commissioner's Office, "Children," ICO, Dec. 10, 2018. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/

[60] M. V. de A. Cunha, "Child privacy in the age of web 2.0 and 3.0: Challenges and opportunities for policy," *Innocenti Discussion Papers,* no. 2017-3, Dec. 2017. [Online]. Available: https://www.unicef-irc.org/publications/pdf/Child_privacy_challenges_opportunities.pdf

[61] UNICEF, "The state of the world's children 2017: Children in a digital world," UNICEF Dec. 2017. [Online]. Available: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf

[62] J. Gligorijević, "Children's privacy: The role of parental control and consent," *Hum. Rights Law Rev.,* vol. 19, no. 2, pp. 201–229, Aug. 2019, doi: 10.1093/hrlr/ngz004.

[63] World Economic Forum, "Generation AI: Establishing global standards for children and AI," 2019. World Economic Forum, Jun. 2019. [Online]. Available: http://www3.weforum.org/docs/WEF_Generation_AI_May_2019_Workshop_Report.pdf

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

[65] Office of the Victorian Information Commissioner, "Artificial intelligence and privacy," OVIC Jun. 2018. [Online]. Available: https://ovic.vic.gov.au/wp-content/uploads/2018/08/AI-Issues-Paper-V1.1.pdf

[66] S. McAleese, M. Johnson, and M. Ladouceur, "Young Canadians speak out: A qualitative research project on privacy and consent," MediaSmarts, Ottawa, ON, CAN, Mar. 2020. [Online]. Available: https://mediasmarts.ca/sites/default/files/publication-report/full/report_young_canadians_speak_out.pdf

[67] M. Bashir, C. Hayes, A. D. Lambert, and J. P. Kesan, "Online privacy and informed consent: The dilemma of information asymmetry," *Proc. Assoc. Inf. Sci. Technol.,* vol. 52, no. 1, pp. 1–10, Nov. 2015, doi: 10.1002/pra2.2015.145052010043.

[68] 5Rights Foundation, "Consultation response: General comment on children's rights in relation to the digital environment," 5Rights Foundation, Oct. 2020. [Online]. Available: https://5rightsfoundation.com/our-work/childrens-rights/uncrc-general-comment.html

[69] A. Young, S. Campo, and S. G. Verhulst, "Responsible data for children: Synthesis report," RD4C, New York, NY, USA, Nov. 2019. [Online]. Available: https://rd4c.org/files/rd4c-report-final.pdf

[70] Children's Commissioner for England, "Who knows what about me? A report on the data collected about children and how it might shape their lives," Children's Commissioner for England, Nov. 2018. [Online]. Available: https://www.childrenscommissioner.gov.uk/digital/who-knows-what-about-me/

[71] R. Calo, "People can be so fake: A new dimension to privacy and technology scholarship," *Penn State Law Rev.,* vol. 114, no. 3, pp. 1–49, 2010. [Online]. Available: https://ssrn.com/abstract=1458637

[72] A. Salles, K. Evers, and M. Farisco, "Anthropomorphism in AI," *AJOB Neurosci.,* vol. 11, no. 2, pp. 88–95, Mar. 2020, doi: 10.1080/21507740.2020.1740350.

[73] "Fuel of the future - Data is giving rise to a new economy," *The Economist,* May 6, 2017. [Online]. Available: https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy

[74] D. Holloway, "Surveillance capitalism and children's data: The Internet of Toys and Things for children," *Media Int. Aust.,* vol. 170, no. 1, pp. 27–36, Feb. 2019, doi: 10.1177/1329878X19828205.

[75] Office of the Privacy Commissioner of Canada,"News release: VTech breach investigation highlights security failures ," OPC, Jan. 8, 2018. [Online]. Available: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/nr-c_180108/

[76] D. Lupton and B. Williamson, "The datafied child: The dataveillance of children and implications for their rights," *New Media Soc.,* vol. 19, no. 5, pp. 780–794, Jan. 2017, doi: 10.1177/1461444816686328.

[77] J. Enriquez, "Are you tattooed … yet?" UNICEF. Available: https://sites.unicef.org/sowc2017/index_102054.html (accessed Nov. 16, 2020).

[78] A. G. Espanol, "Ethical framework for artificial intelligence in Colombia." Presidential Advisory for Economic Affairs and Digital Transformation, Presidency of the Republic of Colombia, Aug. 2020. [Online]. Available: https://dapre.presidencia.gov.co/dapre/SiteAssets/documentos/ETHICAL FRAMEWORK FOR ARTIFICIAL INTELLIGENCE IN COLOMBIA.pdf

[79] European Commission, "White paper on Artificial Intelligence – A European approach to excellence and trust," EC, Feb. 2020. [Online]. Available: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

[80] L. Na, C. Yang, C. C. Lo, F. Zhao, Y. Fukuoka, and A. Aswani, "Feasibility of reidentifying individuals in large national physical activity data sets from which protected health information has been removed with use of machine learning," *JAMA Netw. open,* vol. 1, no. 8, pp. 1-13, Dec. 2018, doi: 10.1001/jamanetworkopen.2018.6040.

[81] International Working Group on Data Protection in Telecommunications, "Working paper on privacy and Artificial Intelligence," IWGDPT, Nov. 2018. [Online]. Available: https://epic.org/IWG/WP-AI.pdf

[82] R. Heilweil, "New surveillance AI can tell schools where students are and where they've been," *Vox,* Jan. 25, 2020. [Online]. Available: https://www.vox.com/recode/2020/1/25/21080749/surveillance-school-artificial-intelligence-facial-recognition

[83] "Ring video doorbells get 15+ million dings this halloween and capture cute costumes and fun pranks," *Ring Blog,* Nov. 4, 2019. [Online]. Available: https://blog.ring.com/2019/11/04/ring-video-doorbells-get-15-million-dings-this-halloween-and-capture-cute-costumes-and-fun-pranks/

[84] V. Steeves and J. Owain, "Editorial: Surveillance, Children and Childhood," *Surveill. Soc.,* vol. 7, no. 3/4, pp. 187–191, 2010, doi: 10.24908/ss.v7i3/4.4151.

[85] Committee on the Rights of the Child, *Draft General Comment No. 25 (202x), Children's rights in relation to the digital environment,* Aug. 13, 2020. [Online]. Available: https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx

[86] V. Barassi, "The human error in AI and question about children's rights: Response to the consultation on the white paper on Artificial Intelligence - A European approach," Child Data Citizen, Jun. 15, 2020. [Online]. Available: http://childdatacitizen.com/human-error-ai-childrens-rights/

[87] Privacy International, "Privacy and freedom of expression in the age of Artificial Intelligence," Privacy International Apr. 2018. [Online]. Available: https://privacyinternational.org/report/1752/privacy-and-freedom-expression-age-artificial-intelligence

[88] FAT/ML, "Fairness, accountability, and transparency in Machine Learning." [Online]. Available: https://www.fatml.org/ (accessed Nov. 29, 2020).

[89] S. Lo Piano, "Ethical principles in machine learning and artificial intelligence: Cases from the field and possible ways forward," *Humanit. Soc. Sci. Commun.,* vol. 7, no. 9, Jun. 2020, doi: 10.1057/s41599-020-0501-9.

[90] F. Z. Borgesius, "Discrimination, artifical intelligence, and algorithmic decision-making," Council of Europe, Strasbourg, France, Feb. 2019. [Online]. Available: https://www.coe.int/en/web/european-commission-against-racism-and-intolerance/-/-discrimination-artificial-intelligence-and-algorithmic-decision-making-

[91] The Algorithmic Justice League,"Library of content," AJL. [Online]. Available: https://www.ajl.org/library/home (accessed Nov. 29, 2020).

[92] N. Singer and C. Metz, "Many facial-recognition systems are biased, says U.S. study," *The New York Times,* Dec. 19, 2019. [Online]. Available: https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html?searchResultPosition=1

[93] S. Jemielity, "Health care prediction algorithm biased against black patients, study finds," *UChicago News,* Oct. 28, 2019. [Online]. Available: https://news.uchicago.edu/story/health-care-prediction-algorithm-biased-against-black-patients-study-finds

[94] C. F. Kerry, "Protecting privacy in an AI-driven world," Brookings Institution, Washington, DC, Feb. 10, 2020. [Online]. Available: https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/

[95] Bahador Khalegi, "The why of explainable AI," *Element AI,* Aug. 19, 2019. [Online]. Available: https://www.elementai.com/news/2019/the-why-of-explainable-ai

[96] D. Dawson et al., "Artifical intelligence: Australia's ethics framework," Data 61CSIRO, Australia, 2019. [Online]. Available: https://consult.industry.gov.au/strategic-policy/artificial-intelligence-ethics-framework/supporting_documents/ArtificialIntelligenceethicsframeworkdiscussionpaper.pdf

[97] Office of the Privacy Commissioner of Canada, "A regulatory framework for AI: Recommendations for PIPEDA reform," *OPC,* Nov. 12, 2020. [Online]. Available: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/reg-fw_202011/

[98] Freedom Online Coalition, "FOC joint statement on Artificial Intelligence and human rights," Government of Canada, Nov. 3, 2020. [Online]. Available: https://www.international.gc.ca/global-affairs-affaires-mondiales/news-nouvelles/2020/2020-11-05-internet-freedom-liberte-internet.aspx?lang=eng

[99] U. Gasser, "AI innovators should be listening to kids," *Wired,* Nov. 26, 2019. [Online]. Available: https://www.wired.com/story/ai-innovators-should-be-listening-to-kids/

[100] A. Cavoukian, *Privacy by Design: The 7 Foundational Principles,* Information and Privacy Commissioner of Ontario, Toronto, ON, CAN, Jan. 2011. [Online]. Available: https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf

[101] Element AI, "Closing the human rights gap in AI governance," Element AI, Nov. 2019. [Online]. Available: http://mediaethics.ca/closing-the-human-rights-gap-in-ai-governance/

[102] R. Davidson, K. Schuller, and M. Matthews, *Harnessing the Benefits of AI while Reducing the Harms, Information and Communications Technology Council,* Ottawa, ON, CAN, Mar. 2020. [Online]. Available: https://www.ictc-ctic.ca/wp-content/uploads/2020/05/OPC-Consult-English.pdf

[103] Information Commissioner's Office, "What is the Children's Code?" ICO. [Online]. Available: https://ico.org.uk/for-organisations/age-appropriate-design/additional-resources/what-is-the-children-s-code/ (accessed Jan. 13, 2021).

[104] K. Pylypczuk, "UK draft code for children's privacy has broad scope, could influence Canadian approach," *Dentons Data,* Jun. 3, 2019. [Online]. Available: http://www.dentonsdata.com/uk-draft-code-for-childrens-privacy-has-broad-scope-could-influence-canadian-approach/

[105] Information Commissioner's Office, "Age appropriate design: A code of practice for online services," ICO, Sep. 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/

[106] Ontario Society of Professional Engineers, "Office of the Privacy Commissioner of Canada's consultation on artificial intelligence," OSPE, Mar. 2020. [Online]. Available: https://ospe.on.ca/wp-content/uploads/2020/03/Office-of-the-Privacy-Commissioner-of-Canadas-Consultation-on-Artificial-Intelligence.pdf

[107] UNICEF Office of Global Insight and Policy, "Workshop report: AI and child rights policy," UNICEF, Sep. 2019. [Online]. Available: https://www.unicef.org/globalinsight/media/661/file

[108] K. Alwani and M. C. Urban, *The Digital Age: Exploring the Role of Standards for Data Governance, Artificial Intelligence and Emerging Platforms,* CSA Group, Toronto, ON, CAN, May 2019. [Online]. Available: https://www.csagroup.org/wp-content/uploads/CSA-Group-research-Digital-Economy.pdf

[109] Jonathan P. How, "Ethically aligned design [From the Editor]," *IEEE Cont. Sys. Mag.,* vol. 38, no. 3, pp. 3-4, Jun. 2018, doi: 10.1109/MCS.2018.2810458.

[110] 5Rights Foundation, "Standard for an age appropriate digital services framework." 5Rights Foundation. [Online]. Available: https://5rightsfoundation.com/our-work/design-of-service/standard-for-an-age-appropriate-digital-services-framework.html (accessed Nov. 30, 2020).

[111] Information Commissioner's Office, "Guide to the General Data Protection Regulation (GDPR)," ICO, Jan. 2021. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

[112] S. Livingstone, M. Stoilova, and R. Nandagiri, "What's the role of the school in educating children in a datafied society?" *London School of Economics Blog,* Oct. 23, 2019. [Online]. Available: https://blogs.lse.ac.uk/parenting4digitalfuture/2019/10/23/whats-the-role-of-the-school-in-educating-children-in-a-datafied-society/

[113] United Nations Educational, Scientific and Cultural Organization, "Beijing consensus on artificial intelligence and education," UNESCO, May 2019. [Online]. Available: https://unesdoc.unesco.org/ark:/48223/pf0000368303

[114] MediaSmarts, "Digital literacy 101," MediaSmarts. [Online]. Available: https://mediasmarts.ca/teacher-resources/digital-literacy-101 (accessed Sep. 18, 2020).

[115] Kids Code Jeunesse,"The algorithm literacy project." [Online]. Available: https://algorithmliteracy.org/ (accessed Nov. 29, 2020).

[116] Office of the Privacy Commissioner of Canada, "Real fears, real solutions: A plan for restoring confidence in Canada's privacy regime," OPC, Sep. 21, 2017. [Online]. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1

[117] K. Litman-Navarro, "We read 150 privacy policies. They were an incomprehensible disaster," *The New York Times,* Jul. 12, 2019. [Online]. Available: https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html

[118] L. Fadrique, A. Kuang, L. U. Mazza, and P. P. Morita, *Rethinking Privacy Agreements,* CSA Group, Toronto, ON, CAN, Mar. 2020. [Online]. Available: https://www.csagroup.org/wp-content/uploads/CSA-Group-Research-Privacy-Agreements.pdf

[119] Interactive Advertising Bureau of Canada, "Submission on the Office of the Privacy Commissioner's proposals for ensuring appropriate regulation on artificial intelligence," IAB Canada, Mar. 11, 2020. [Online]. Available: http://www.iabcanada.com/content/uploads/2020/03/IABOPCAI_MAR11.pdf

[120] Institute of Electrical and Electronics Engineers Standards Association, "The Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS)." [Online]. Available: https://standards.ieee.org/industry-connections/ecpais.html (accessed Jan. 12, 2021).

[121] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder, "A 'nutrition label' for privacy," in *SOUPS 2009: Proc. 5th Symp. Usable Privacy and Secur.,* 2009, no. 4, pp. 1-12, doi: 10.1145/1572532.1572538.

[122] Y. Shen and P. A. Vervier, "IoT security and privacy labels," in *Privacy Technologies and Policy: 7th Annu. Privacy Forum, 2019,* pp. 136–147, doi: 10.1007/978-3-030-21752-5_9.

[123] A. Ahmed, "Apple is introducing 'privacy labels' that will indicate how much data your applications collect," *Digital Information World,* Jun. 24, 2020. [Online]. Available: https://www.digitalinformationworld.com/2020/06/apple-is-introducing-privacy-labels-that-will-indicate-how-much-data-your-applications-collect.html

[124] "Apple starts applying new data privacy labels to apps," *Reuters,* Dec. 14, 2020. [Online]. Available: https://www.reuters.com/article/us-apple-privacy/apple-starts-applying-new-data-privacy-labels-to-apps-idUKKBN28O2KQ?edition-redirect=uk

[125] L. H. Newman, "IoT security is a mess. Privacy 'nutrition' labels could help," *WIRED,* Jun. 9, 2020. [Online]. Available: https://www.wired.com/story/iot-security-privacy-labels/

[126] Internet Society, "Enhancing IoT security: Final outcomes and recommendations report," Internet Society, May 28, 2019. [Online]. Available: https://www.internetsociety.org/resources/doc/2019/enhancing-iot-security-final-outcomes-and-recommendations-report/

[127] BC Freedom of Information and Privacy Association, "The right to erasure," *FIPA,* Feb. 25, 2020. [Online]. Available: https://fipa.bc.ca/the-right-to-erasure/

[128] E. Fosch Villaronga, P. Kieseberg, and T. Li, "Humans forget, machines remember: Artificial Intelligence and the right to be forgotten," *Comput. Secur. Law Rev.,* pp. 1-19, Aug. 2017. [Online]. Available: https://ssrn.com/abstract=3018186

[129] Office of the Privacy Commissioner of Canada, "Tips for using privacy settings," *OPC,* Mar. 5, 2019. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/gd_ps_201903/?WT.ac=set-en-1

[130] Global Privacy Assembly, 42nd Clossed Session, *Resolution on Accountability in the Development and Use of Artifical Intelligence,* Oct. 2020. [Online]. Available: https://globalprivacyassembly.org/wp-content/uploads/2020/10/FINAL-GPA-Resolution-on-Accountability-in-the-Development-and-Use-of-AI-EN.pdf

[131] L. A. Wasser, "How should AI be regulated in Canada? Speak now, or forever hold your peace!" McMillan, Feb. 2020. [Online]. Available: https://mcmillan.ca/insights/how-should-ai-be-regulated-in-canada-speak-now-or-forever-hold-your-peace/

[132] Office of the Privacy Commissioner of Canada, "Statement from the Privacy Commissioner of Canada following the tabling of Bill C-11," OPC, Nov. 19, 2020. [Online]. Available: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/s-d_201119/

[133] "California voters pass the California Privacy Rights Act of 2020," *Cyber/Data/Privacy Insights,* Nov. 4, 2020. [Online]. Available: https://cdp.cooley.com/california-voters-pass-the-california-privacy-rights-act-of-2020/

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™