unicef
for every child

The Case for Better Governance of Children's Data: A Manifesto

Subscribe to OGIP's newsletter **New Insights** to see how our expectations and recommendations evolve over time

Contents

Acknowledgements

This Manifesto is the product of a year-long process and the collective wisdom and work of 17 global experts who formed the Data Governance Working Group and provided analysis, insights, guidance and comments to inform the final report. These are:

Lindsey Barrett, Georgetown Law

Monica Bulger, Joan Ganz Cooney Center at Sesame Workshop

Heather Burns, Open Rights Group

Jasmina Byrne, UNICEF, Office of Global Insight and Policy

Jeff Chester, Center for Digital Democracy

Emma Day, UNICEF

Steven Feldstein, Carnegie Endowment for International Peace

Urs Gasser, Berkman Klein Center for Internet & Society

Jay Harman, formerly 5Rights

Pedro Hartung, Alana Institute

Malavika Jayaram, Digital Asia Hub

Sean McDonald, Digital Public

Linda Raftree, Independent Consultant

Nanjira Sambuli, Researcher, Policy Analyst and Advocacy Strategist

Caroline Sinders, Convocation Design

Steven Vosloo, UNICEF, Office of Global Insight and Policy

Andrew Young, The GovLab

This document was also informed by three rounds of consultation organized by the Berkman Klein Centre for Internet & Society, Alana Institute from Brazil and UNICEF covering the following regions –Africa, Asia, Europe, Latin America and North America. Over 100 experts from various institutions, organizations and companies contributed through these consultations and informal interviews. The team is particularly grateful to those who have provided additional written comments: MyData Global/ #MyData4Children group, Riitta Vänskä, Tiina Härkönen and Reijo Aarnio (SITRA Finland), Tim Unwin (Royal Holloway, University of London), Alexandre Barbosa and Fabio Senne (Cetic.br), Council of Europe's Children's Rights Division and Data Protection Unit, Sonia Livingstone (London School of Economics), Anri van der Spuy (Research ITC Africa), Eddan Katz (World Economic Forum), Bushra Ebadi, Gabrielle Berman, Karen Carter, Afrooz Johnson, Sigrun Kaland, Josianne Galea Baron, Melanie Penagos and Sarah Jacobstein (UNICEF).

The Manifesto was produced by UNICEF's Office of Global Insight and Policy under the leadership of Laurence Christian Chandy (Director) and Jasmina Byrne (Chief of Policy). The report was authored by Jasmina Byrne, Emma Day (UNICEF) and Linda Raftree (independent consultant).

This document was copy-edited by Eve Leckey while art direction was provided by Mariana Amaral, design by Mardiyah Miller and maps by Gabrielle Mérite.

This document is interactive and designed for digital viewing.

Please consider the environment and refrain from printing.

Data, if used responsibly, can solve social problems and challenges while offering tremendous potential for innovation. This is as true for children as it is for adults.

Key Messages:

Children, however, are more vulnerable than adults and are less able to understand the long-term implications of consenting to their data collection. Existing privacy and fairness concerns stemming from the collection of adults' data are magnified when it comes to the collection of data from children, given their greater cognitive, emotional, and physical vulnerabilities.

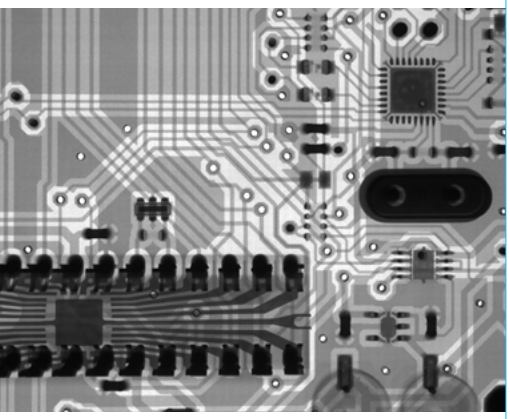
The implications of surveillance and tracking are also more significant for children due to greater exposure over their lifetime, and due to the importance of childhood as a time for development and experimentation with identity. How data are collected, stored and processed affects how data are then used to inform decisions that affect children's current and future lives.

As all areas of children's lives become increasingly enmeshed with digital technologies, it is possible to envision a future in which these technological advancements are primarily applied in service of children and their communities.

To achieve this future, guiderails and benchmarks need to be established that will help govern children's data in a responsible way. This means that harnessing of data for social good can't come at the expense of children's privacy, protection, or well-being. It also means that the benefits of data collection and use should be spread evenly across the developed and developing world.

Better data governance for children, with clear duties, standards and responsibilities, is critical to ensure that children are protected, and that data are used as a force for good for generations to come.

The hurdles standing in the way of better governance of children's data are many and complex, and they have been allowed to grow largely unchallenged as data have come to play a growing role in children's lives.



What are the challenges?

- **Surveillance culture threatens children's freedom and privacy.** Surveillance by corporations and governments can have a chilling effect on children at a key development stage, and the permanence of data can have a negative impact on their futures.
- **Poor protection of children's sensitive data paves the way for even more surveillance and use in unanticipated and harmful ways.** The lack of clear regulation, standards, and limits on how children's data are managed – including the commercialization of these data – creates both short- and long-term risks.
- **Predictive analytics can amplify existing discrimination and bias.** Artificial Intelligence is increasingly used to make critical decisions for children, such as allocation of welfare benefits or where schools should be built. When these systems use biased data sets, discrimination can result.
- **Children's data can be used to manipulate and influence their behaviour.** Civil society organizations, governments and social media platforms increasingly deploy 'microtargeting' to shape children's beliefs on issues such as gender or political participation. Children are highly susceptible to these techniques which, if used for harmful goals, are unethical and undermine children's freedom of expression.

- **Legal frameworks generally overlook the risks for children of group data profiling.** Social media companies, for example, use children's data to group them into segments and micro target them with advertising. Such group data, if exploited, can reveal characteristics, attributes, and locations of children. Aggregated, non-personal data need further exploration and adequate regulation.

- **Balancing conflicting rights is challenging.** Emerging tensions between seemingly conflicting rights – for example, protection and privacy – can be difficult to reconcile. Issues such as age verification, encryption and use of parental controls must be considered in connection with children's wishes, capacities and freedoms.

- **Data governance does not account for children's evolving capacities and different experiences.** Children and adolescents have differing levels of awareness of what information is collected online and for what purposes. But data privacy laws and policies at best treat children as a homogeneous group.

- **Most data regimes do not adequately address consent, child protection and representation.** Using age to indicate that a child can understand terms and conditions and consent to data collection may not be meaningful or appropriate. In addition, the internet makes it tough to obtain parental consent, while current consent frameworks may lead to parents and guardians overriding children's rights to freedom of expression and participation.

These ten actions form a Manifesto that articulates a vision for a better approach to children's data. The international community must consider these actions when developing and implementing data governance frameworks.

1.

PROTECT children and their rights through child-centred data governance. Such data governance should adhere to internationally agreed standards that minimize the use of surveillance and algorithms for profiling children's behaviour.

2.

PRIORITIZE children's best interests in all decisions about children's data. Governments and companies should give priority to children's rights in their data collection, and processing and storage practices.

3.

CONSIDER children's unique identities, evolving capacities and circumstances in data governance frameworks. Every child is different and children mature as they get older, so data governance regulations must be flexible. Marginalised children must never be left behind.

4.

SHIFT responsibility for data protection from children to companies and governments. Extend the protection measures to all children below the age of 18, regardless of the age of consent.

5.

COLLABORATE with children and their communities in policy building and management of their data. Through distributed models of data governance, children and their communities should have more say in how data is processed, by whom it can be processed, and with whom it can be shared.

6.

REPRESENT children's interests within administrative and judicial processes, as well as redress mechanisms. It is imperative that children's rights are integrated into existing mechanisms, such as the work of data protection authorities.

7.

PROVIDE adequate resources to implement child-inclusive data governance frameworks. Data protection authorities and technology companies must employ staff who understand children's rights, and governments should allocate funding for regulatory oversight.

8.

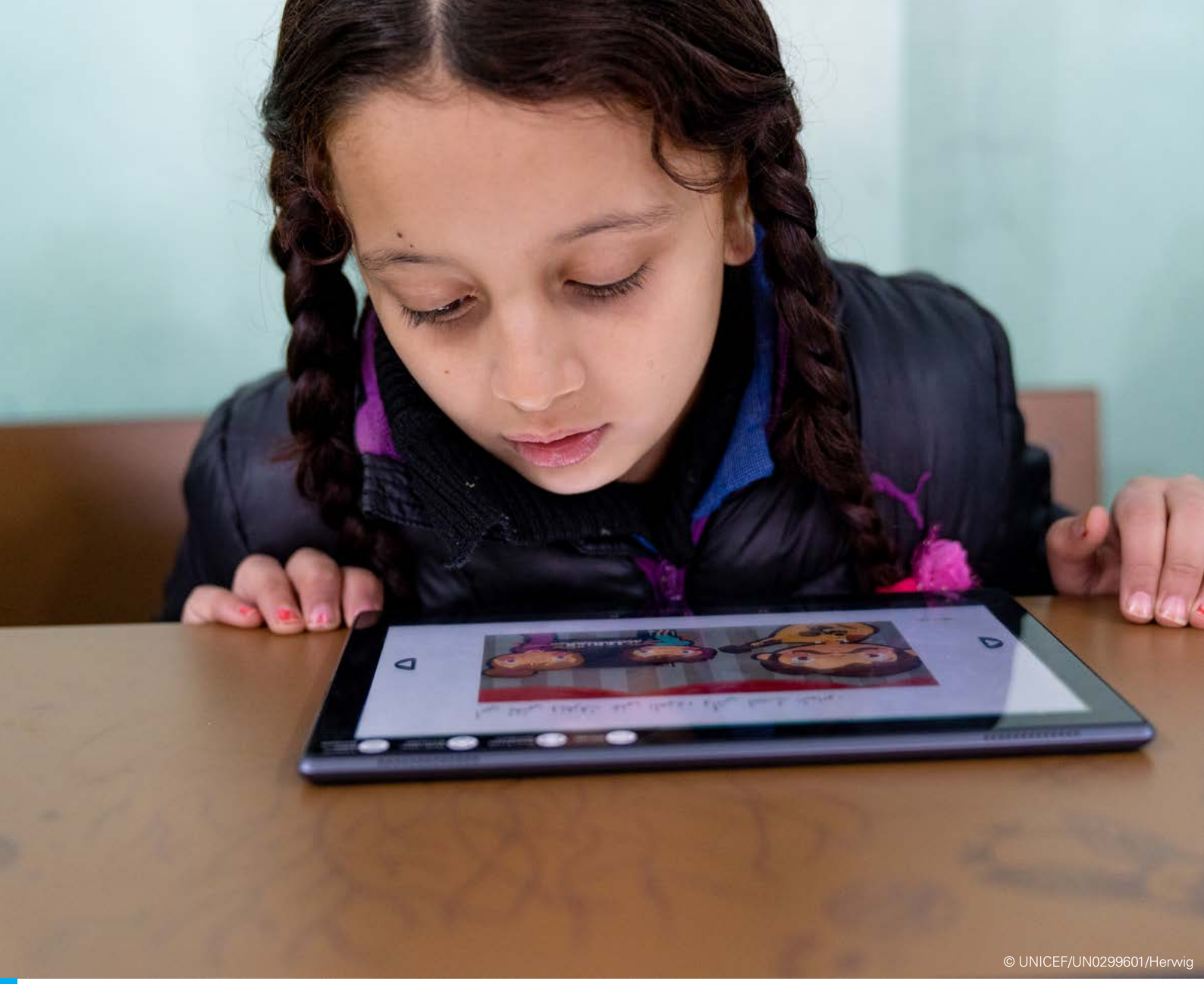
USE policy innovation in data governance to solve complex problems and accelerate results for children. Policy innovation can help public authorities to make the most of data, while at the same time safeguarding children's rights.

9.

BRIDGE knowledge gaps in the realm of data governance for children. There are some urgent knowledge gaps that need further research to ensure that data governance regulations are evidence-based.

10.

STRENGTHEN international collaboration for children's data governance and promote knowledge and policy transfer among countries. This Manifesto calls for greater global coordination on law and policy. Uncoordinated national-level data governance laws can lead to competing assertions of jurisdiction and conflict.



© UNICEF/UN0299601/Herwig

Introduction

By the time a child turns 18, tens of thousands of data points will have been collected about them.[2]

Why a Manifesto on children's data governance?

How do we define children?

The UN Convention on the Rights of the Child defines children as those under the age of 18.[1]

Children's data are captured and used in a multitude of ways in both high-tech and low-tech societies – from the time they are in the womb, when some parents capture and share ultrasound images – to adulthood. From the earliest possible ages children's photos and other data are digitized and uploaded to the internet. They are observed by parents as well as private companies through baby cameras and toys embedded with data-generating sensors. As they grow older, children use mobile devices for entertainment, including educational games and videos. As pre-teens and teenagers, children access social media, messaging apps, and other platforms and channels that help them stay connected with their peers, teachers and the wider world. Companies that manage these platforms, and third parties who have access to these data, have an exclusive view into their lives and habits.

© UNICEF/UN0309991/Arcos

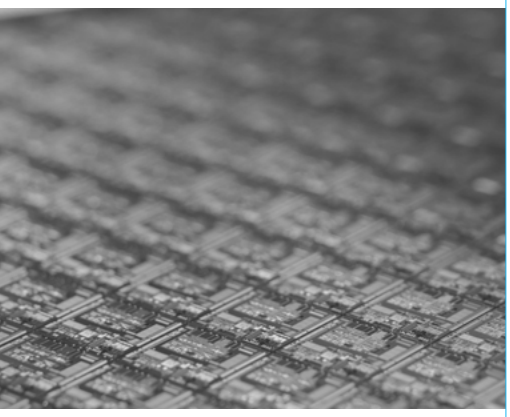
What are personal data?

Personal data are defined as any information that relates to an identified or identifiable living individual.[3] 'Personal data' under the General Data Protection Regulation (GDPR) and as defined by the Child Online Privacy Protection Act (COPPA) includes online identifiers such as device ID, IP address, cookies, geolocation information, photos, videos, audio recordings, browser type and plug-in details.[4,5] Personal data also includes different pieces of information which, when collected together, could identify a particular person, and any data that have been de-identified but could be used to re-identify a person. For data to be truly anonymous the anonymization must be irreversible.

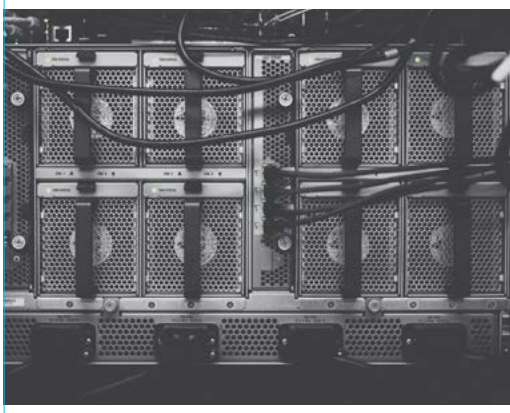
Governments too collect data about children – from the increasing use of biometric technology in birth registration, through to inclusion in public sector data systems, school records, health tracking systems, and national ID systems. In contexts where basic services are not delivered by government, data is also collected by NGOs, international organizations and UN agencies. Some groups of children such as children on the move, children in alternative care, and children in conflict with the law, may be subject to more data collection than others.

Data, if used responsibly, can have transformative power for solving social problems and can offer tremendous potential for innovation. Data collection and processing at scale now underpin many health, education and social services used for and by children. This information is often used to make assessments and determinations of children's needs, abilities and future prospects. Data collected from and about children also provide a rich evidence base from which companies and governments can improve their effectiveness and efficiency.

The challenge we are facing today, during a period of exponential growth of data, is how to maximize the benefits gleaned from data, while at the same time ensuring that individuals, including children, are protected, empowered and endowed with control over their personal data and knowledge of their use. We hope that the future offers a scenario where data from and about children is used solely and exclusively for their benefit – for example, to identify their potentials or their vulnerabilities and to help us offer better targeted support and preventative services.



We believe that children's data merit special protection and a distinct consideration in international and national governance regimes. Misuse of children's data violates their rights under the UN Convention on the Rights of the Child (CRC). Respect for and implementation of these rights as we move further into the digital age are not only legal and moral imperatives, but also represent an important step towards ensuring children's psychological and physical well-being.[6] States, companies and guardians have a duty under existing international human rights laws to prevent children's personal information and data from being used to exploit them or violate their freedoms.



The main difference between general data governance and children's data governance is the presumption that children cannot effectively advance and advocate on behalf of their own interests because of their age and capacity.[7] We outline four key reasons why specific consideration should be given to children:

- Childhood is a period of growth and experimentation, and children's choices and preferences shift and change as they explore their worlds and their identities. Privacy and protection of their identity and their information enables them to develop their personalities.

- Children are a group with limited autonomy which, depending on their age and evolving capacities, makes them less suited than adults to provide meaningful consent for their data collection and use. Even when children and those around them know that their data are being collected, they often do not have clarity about how these data are used, by whom, for what purposes, nor do they have a meaningful ability to respond to potential negative consequences of data use. Governments, businesses and public/private welfare bodies all have responsibilities in relation to children and their data. However, the power imbalance that exists in the physical and the digital world, such as the power disparity between a child and an adult, a large corporation and an individual, or government and citizen, places children in an especially vulnerable position.

- Children generally care about the collection and use of their data, but feel they do not have a choice in decisions about how their data are collected and used. Evidence shows that children have different levels of awareness that online disclosure of information has privacy consequences.[8] They continuously navigate between the desire to engage with others and the desire to protect themselves. However, even when they are careful with the data they share, children have little control over the data others (parents, peers) share about them and how their data are used by third parties, leading to a seemingly ambivalent or resigned attitude to data privacy.[9]

- Insights derived from children's data can support research, development and provision of services, thus poor data governance may lead to loss of potential benefits for children. Good governance of children's data is not only beneficial for them, it can be beneficial for development, business and a data-driven economy.

What is data governance?

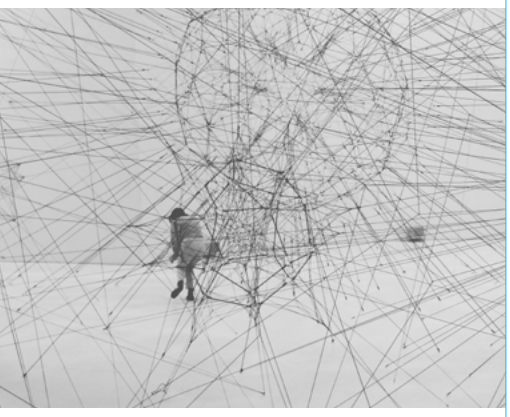
Data governance encompasses the universe of rules and norms that dictate why and how data are captured and used and who holds responsibility for the process. Beyond data management, data privacy, or even data protection, data governance includes policy, strategies, standards, rights and accountability for the end-to-end cycle of data.

This document has a dual aim: first, to raise awareness of the issues specific to children's data by analysing the current status and pointing to key gaps in policy and practice; and **second,** to encourage governments, businesses and public/private welfare bodies to specifically address children's rights within existing and future data governance frameworks.

With a growing number of countries introducing data protection regulation, we have an opportunity to bring about positive change that benefits the youngest members of society. Better data governance for children, with clear duties, standards and responsibilities that span the full ecosystem of data, is critical to ensure children are protected from data misuse and resulting harms, and that data are used as a force for good for generations to come.

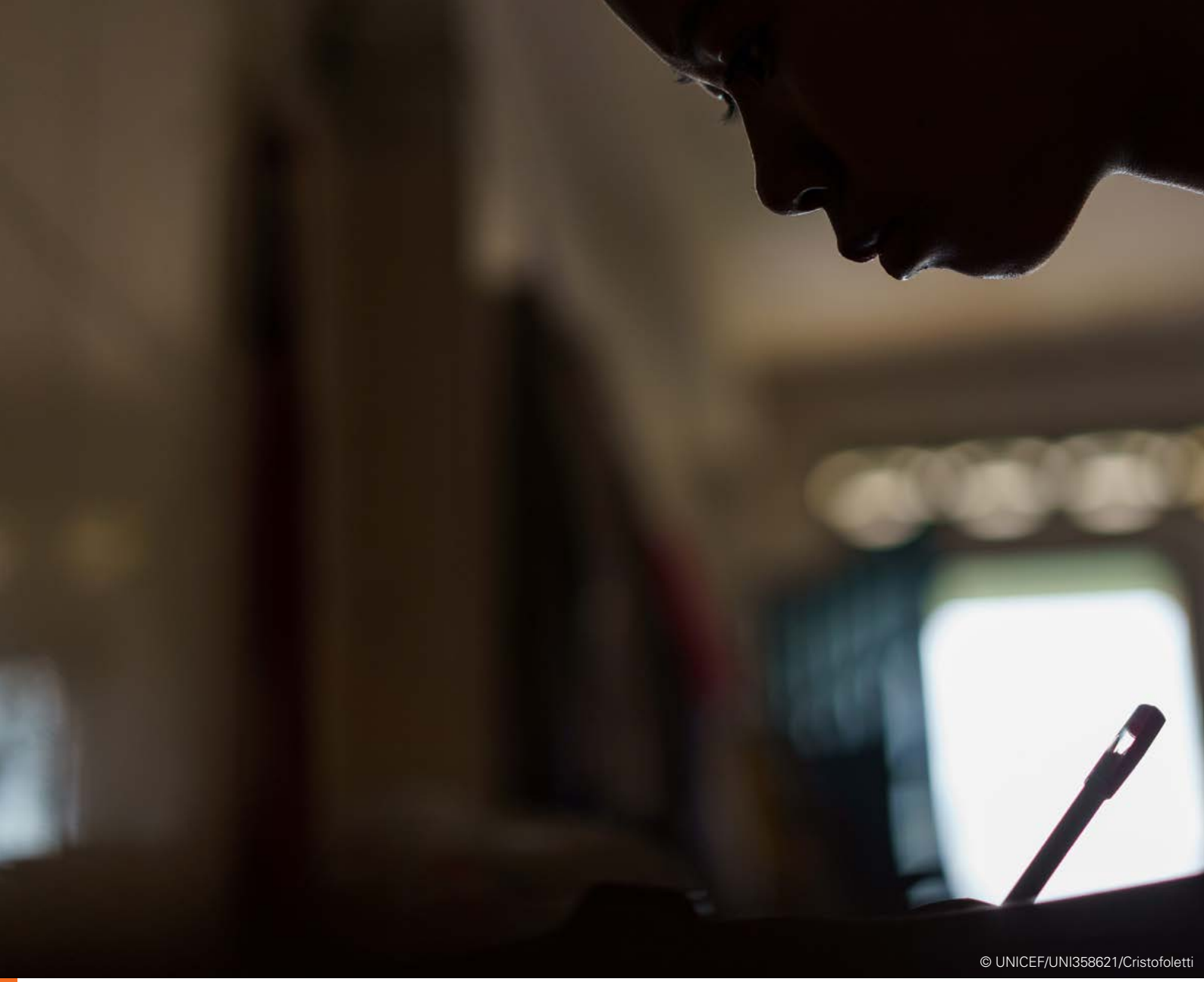
© UNICEF/UN063143/Altaf Ahmad

UNICEF's Office of Global Insight and Policy worked with a group of 17 global experts from a range of disciplines and perspectives to explore trends in the governance of children's data, including the tensions between different rules and norms, emerging concepts and practice, and implications for policy and regulation.



How was the Manifesto developed?

Members of the working group developed a set of background papers exploring a wide range of issues related to children's data governance, including marketing and advertising to children, state surveillance of children through their data, education and health surveillance data, group profiling and demographically identifiable information, the potential role for data fiduciaries, the right to be forgotten, and models for a child-rights-by-design approach for technology companies. We drew from these papers as well as from working group discussions and debate. We also curated information and ideas from diverse sources, including existing literature and policy documents, media reports related to data governance, key informant interviews, events and online meetings, and other sources. Finally, we shared the draft findings and recommendations with more than 100 experts through online workshops and meetings, whose valuable insights have helped shape this final version of the Manifesto.

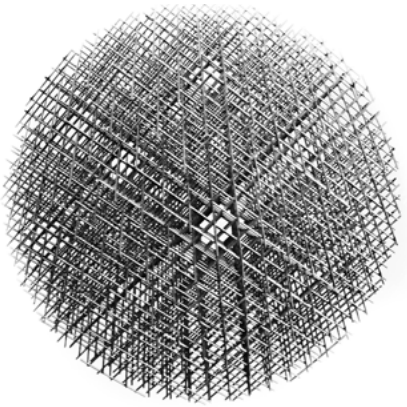


© UNICEF/UNI358621/Cristofoletti

PART 1

Children's data and their rights

Numerous actors collect and share children's data for a multitude of purposes, in ways that are often so seamless that neither children nor their adult guardians are aware that their data are being captured and processed.



The ecosystem of children's digital data

The digital data ecosystem is complex and intertwined with every part of a child's life. While details change according to the context, the data ecosystem has several key players.

- **Governments,** including various agencies, enact laws and regulations related to data processing and use; collect, process, share, store children's data; and use data to make public policy decisions about and for children.

- **Private sector companies and platforms** collect, process, share, store children's data; make decisions about how children's data will be collected, processed, shared, used and maintained and in which systems; and use children's data to make business decisions. Data collected from users of social media platforms, including children, come from registration and login details, online activity, content produced by users and information generated from personal devices.[10]

- **Data brokers** are third party companies that collect data points about individuals (age and gender, interests, education level, state of health, religion and other) and create user segments or profiles which they sell to companies.[11] Data brokers often operate behind the scenes and are outside the control of individuals using these online platforms and services.

- **Non-profit organizations** collect, aggregate, process, share children's data; make decisions about how data will be collected, processed, shared, used and maintained and in which system; and make decisions on services offered to children.

- **Parents and guardians** generate and share children's data, and act as proxies for their children when consenting to children's data use.

- **Children** create data points about themselves and their peers, they share their data with others, and consent to their data being processed.

These actors do not operate in isolation and data often flow between multiple actors. The lines between these actors, often in public-private partnerships, makes data governance and accountability challenging. Nevertheless, all these entities, regardless of their role along the data life cycle, are responsible for protecting children's data and upholding children's rights. Some examples of children's data flow are below:

- **A school** might mandate the use of an online child safeguarding program on both school-issued devices and student personal devices. The software, designed by private companies to surveil children's web searches, might also enable teachers to monitor what children type in real time, and match this with a list of thousands of words that can indicate harmful behaviours, such as abuse, self-harm, violence or extremism. Data from this kind of safeguarding software can be used to refer children to a government intervention or a watchlist.[12]


© UNICEF/UN0410299/Tinago

- **A government** might share or sell its population's health data to a commercial data analytics firm to generate insights to plan a national health strategy.[13] The commercial firm might build a profitable commercial health algorithm using this data, or it might sell data models to health insurance companies to predict who will be healthy or sick.

- **A private sector platform** might share video footage from a home security camera system or public spaces that children frequent with law enforcement or government authorities, regardless of whether a person captured by the camera has given their consent or if the individual is a child.[14]

- **A non-profit organization** might develop a wearable digital necklace for infants, initially for the purpose of reducing child mortality by tracking immunizations. The uses of the tool might then be expanded to include the collection of biometric information from babies, mothers and health workers, and several private sector actors might be brought in across different countries, with whom data would be shared, used, and re-used.[15]

Sitra Digitrail Survey[16]

A two-week study of the online data flows of six individuals carried out by Sitra, an independent public foundation from Finland, illustrates the complexity of this ecosystem. The aim of the study was to find out how much data is being collected from each individual and which third party companies have access to the data. Test subjects included a 16-year-old boy, a student, a politician, a journalist, a company director and a retiree. The study uncovered a host of second and third parties behind the services that the test subjects used directly. One website, for example, shared data with 56 different parties. Test subjects were aware that they had approved some level of data collection by using an online service, but they were surprised by the names and number of the third parties that also had access to their data. Unsurprisingly, they had not read the terms and conditions and cookie settings for the services that they used.

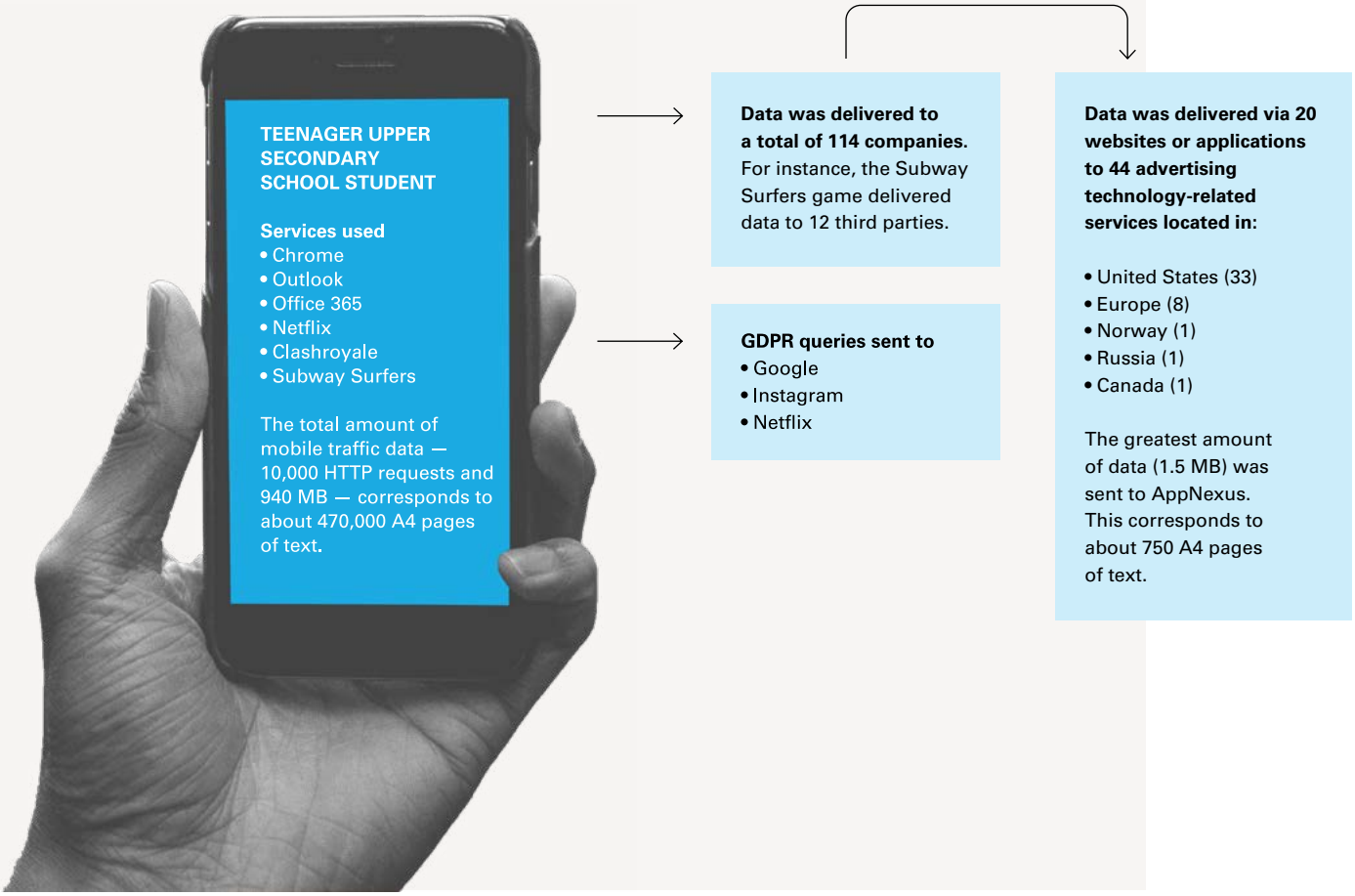
The 16-year-old boy's data were transmitted to 114 companies and a total of 44 advertising companies, the largest amount of data of all the study subjects. The actual number of websites using advertising technology was likely higher, considering that not all of the packets sent to advertising servers provided

reference values indicating the website to which the request was related. The type of data collected by Google about the boy included: profile data, phone configuration, information on the phone's application store, browser settings, location history, stored locations, task lists, YouTube searches and viewing history, and other data related to his Gmail account. Test subjects sent a query to other service providers to ask what data were being collected about them and how they were being profiled (a right afforded by the GDPR), yet these companies did not respond.

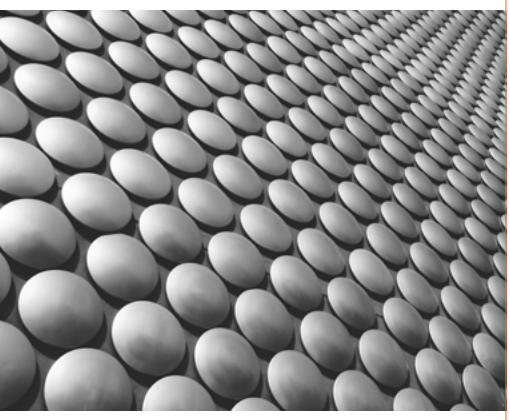
This small-scale case study is just one illustration of the immense volume of data points collected on children and the monetary value placed on children's data, in particular by advertising agencies.

According to Sitra's digiprofile test[17] taken by around 20,000 individuals, young people below 20 years old and the over-65 population had similar, limited levels of knowledge about the basics of data economy, online data protection, and trust towards digital service providers.

FIGURE 1 THE UPPER SECONDARY SCHOOL STUDENT'S DATA WAS TRANSMITTED TO 114 ACTORS



The United Nations Convention on the Rights of the Child (CRC) is one of the most comprehensive and most broadly ratified treaties in the world.



A child rights framework in the data context

While it was adopted more than 30 years ago, its universal and forward-looking principles and provisions are deeply relevant today. While the Convention is not a legally binding instrument on the business sector, it recognizes the responsibilities of private actors to respect children's rights.[18] Further to Article 3.1 of the CRC, and General Comment No. 16, all decisions made by States Parties or by private actors, including business enterprises in the digital environment, and both public and private welfare organizations, should consider children's evolving capacities, their best interests, and the promotion and protection of all their rights. The relevance to and applicability of the Convention on the digital environment is fully laid out in General Comment No. 25, which we explore in greater depth later in this document. The CRC can be directly applied to children's data, as summarized below:[19]

- **The right not to be discriminated against (Article 2)**
  Children's data should never be used to discriminate against them negatively or in ways that impact their well-being, access to information, or digital opportunities. When data are used to profile children or for automated decision-making, a careful analysis can help ensure that underlying models are not created with biased data or assumptions.

- **The best interests of the child and the right to be heard (Articles 3 and 12)**
  Children's best interests should be the primary consideration, even in the face of lawful bases for data collection. All actors involved in the children's data system are encouraged to understand how to uphold the best interests of the child even when they seemingly clash with the interests of companies, organizations, or governments.[20] Children have the right to be heard in any processes related to their data and digital experiences and be involved in governance, decision and policymaking and design of products, wherever possible.

- **Age and evolving capacity (Article 5)**
  Childhood, defined as the period between 0 and 18 years of age, is a time when attitudes, preferences and identity are fluid and under formation. The capacity to make informed decisions and to exercise full agency is lower for younger children, presenting unique challenges when it comes to data privacy and to the myriad ways that data are used. The 'evolving capacities of the child' concept means that the direction and guidance, provided by parents or others with responsibility for the child, must take into account the capacities of the child to exercise rights on their own behalf. As children grow and develop, they acquire enhanced competencies, need less direction, and have greater capacity to take responsibility for decisions affecting their lives, including the use of their data.[21]

- **Freedom of expression, freedom of thought, and the right to seek or share information and ideas (Articles 13, 14)**
  Children have the right to freedom of expression, which includes the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers. The use of automated decision-making with opaque algorithms based on children's data, as well as echo chambers and self-referential information bubbles, can have negative consequences for children. Children also have the right to freedom of thought, which prevents the use of non-transparent nudge techniques and persuasive technologies for behavioural modulation and manipulation.

- **The right to privacy (Article 16)**
  Children have the right to private and family life in the digital environment, which includes the protection of their personal data. Without the ability to think, write and communicate in

private, children will choose to self-censor rather than experiment with ideas that bring the risk of social, legal or physical consequences.[22,23] The confidentiality of their correspondence and private communications is vital, and so is full control of their data, and the right to opt out of data collection or to have their data erased at any time. Children have the right to privacy vis-à-vis their governments, private companies, civil society actors, international organizations, and to some extent, from their own parents.

- **The right to be protected from exploitation (Articles 19 and 32)**
  Children have the right to be protected from all forms of physical or mental violence, injury or abuse, negligent treatment, maltreatment or exploitation that may be a consequence of the use of their data. They also have the right to be protected from economic exploitation, including through the monetization of personal data, profiling and automated decision-making, microtargeting of advertising, distribution of child sex abuse images facilitated by persistent identifiers, and unauthorized artistic child labour.[24]

- **The rights to development, health, education, rest, leisure and play (Articles 6, 24, 28, 31)**
  The responsible use of children's data by all actors in the digital environment could favour harmonious, healthy and integrated physical, mental, spiritual, moral and social development. Likewise, children's access to services or information that contribute to their development, health, education and leisure should not be conditioned on their provision of personal data in return.

- **The rights to free expression of identity, assembly, diversity of information sources (Articles 8, 17, 15)**
  The CRC recognizes that children are more vulnerable than adults, and that they are in a stage of discovering and deepening their identities and belief systems. In addition to universal human rights, children have participation and protection rights designed to enable them to express themselves and to explore and experiment safely with ideas and identities without being subjected to surveillance or pressure.[25,26]

See the paper from Working Group Member Pedro Hartung on **The Children's Rights-by-Design Standard for Data Use by Tech Companies**

The full realization of children's rights is a difficult balancing act. It requires harmonization between the child participation principle and the right to freedom of expression, for example, and other rights and principles such as the right to protection and the principle of the best interest of the child.[28]

The term "best interests of the child" broadly describes a child's well-being as determined by a variety of individual circumstances, such as the age, the level of maturity of the child, the presence or absence of parents, the child's environment and experiences. Interpretation and application of the best interest of the child can happen at an individual or collective level.[27]

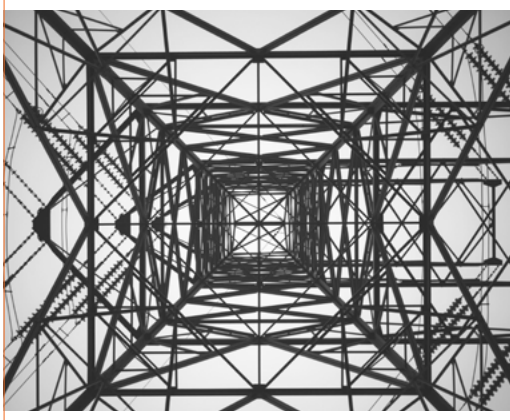
Key areas of concern for children's data governance

Appropriate and responsible use and analysis of data can be beneficial for evidence-based law and policymaking, or as part of ethical research, to improve children's lives. Preventing children from engaging in the online world can curtail their freedoms, while preventing use of their data for development of services may limit opportunities. Children are deprived of their rights through misuse of their data in ways that exploit them, discriminate against them, deny their freedoms, and create societal norms that are unhealthy or damaging.

While this Manifesto focuses on children's data governance, a key point to remember is that many children around the world are not able to enjoy their digital participation rights due to a lack of access to online spaces. UNICEF estimated in 2020 that two-thirds of children and young people aged 25 years or less did not have an internet connection at home. In high-income countries some 87 per cent of children aged 3-17 and young people between 18 and 25 have an internet connection at home, whereas in low-income countries only 6 per cent do. Disparities between rural and urban areas and wealthy and poor households in all countries are also persistent.[29] While being offline means that children are less affected by exploitation of their data, it also means that they are excluded from digital data sets that are driving decision-making, and they might not be able to access online benefits and services.

Key emerging concerns related to the use and processing of children's data are outlined below.

1. Surveillance culture threatens children's freedom and privacy



The collection of multiple data points on children may lead to their surveillance, both as individuals and groups. Their data is gathered by private companies for commercial purposes and by governments as part of national security efforts or for political reasons. Children's data are also captured indirectly because there are few mechanisms that filter children's data out of broad data collection efforts. Once legitimized, this culture of surveillance is difficult to undermine or change.

Children are important targets of the business model that aims to maximize the use of data.[30] Data-driven global marketing and sales systems are embedded into digital platforms and services that are popular with young people. Tracking and targeting software enables access to and analysis of children's personal and consumer data, including information about purchases, devices, online behaviours, location, financial status and health.[31] These data are used to create groups or 'profiles' of users who advertisers target to drive purchases and media consumption, and to influence other online and offline behaviours.[32] By their very design, platforms and applications encourage attachment to social stimulation and the feedback that come through 'liking' and other forms of interaction on social media, all of which leave behind a data trail.[33] While these systems were not created or intended specifically for children, it is important to acknowledge that children are spending most of their time in online spaces intended for adults and that their behaviours are tracked as though they are older.

These advertising and marketing practices raise significant concerns about exposure to advertising itself, as well as to collection, storage and the present and future use of children's digital data. They also point to issues related to the monetization and use of children's personal data. In addition to potentially exposing children to harmful and inappropriate products such as unhealthy food, these marketing techniques are used to manipulate children's consumption patterns and behaviours, thus infringing on their freedom of choice and

See the paper from Working Group affiliates Katherine Montgomery, Jeffrey Chester and Katarina Kopp for more information and recommendations on **Data Governance for Young People in the Commercialized Environment**

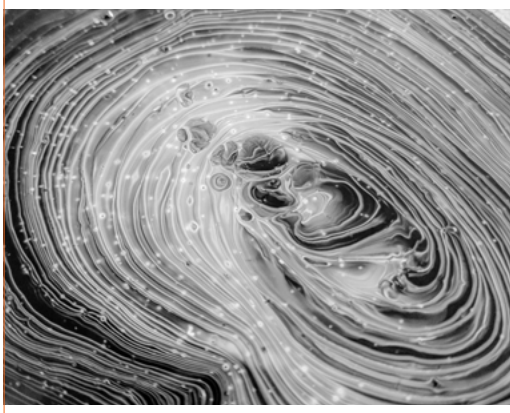
expression. Compounding these problems, the regulatory frameworks to address child privacy and data protection in the commercial digital environment are nascent, fragmented and limited to children below a certain age group – usually 13 or 16 years old where the Children's Online Privacy Protection Act (COPPA, United States) or General Data Protection Regulation (GDPR, European Union) apply.[34]

Surveillance is also a core strategy that governments use to monitor their populations, exert control, address security concerns and establish a desired public order. State surveillance is not a new phenomenon, but new and ever cheaper systems for collecting and processing data have made state surveillance easier and less expensive.[35] On the one hand, commercial tracking and monitoring tactics have been adapted by States to surveil their populations, on the other hand, military communication and surveillance technologies have been adapted for commercial use. While some state surveillance can be legitimate, for example, public safety, national security, and disease tracking and monitoring, these measures are often implemented without much regard for human rights, the right to privacy and freedom of expression, or the rights of association and assembly.[36] Many of these new surveillance technologies develop faster than the legislative frameworks that should govern them.[37]

Strategies that governments employ to surveil their populations range from the use of artificial intelligence (AI) and big data surveillance tools, to passive or targeted surveillance. While children are considered a protected group because of their maturity and capacities, the law grants them little or no protection from government surveillance. Given that children and young people rely heavily on digital platforms to organize themselves and participate in civic life, government surveillance affects their right to freedom of expression and peaceful assembly. According to their maturity and capacity, children may be more or less able to understand the potential implications of surveillance when they make choices about activities in which they participate, where surveillance might be active, or about the risks of being included in broader population sets. The effects of this increased surveillance can follow children throughout their lives. They might be detained for protesting due to the greater capacities of these surveillance tools to identify and locate individuals, leading to deprivation of liberty and a permanent criminal record. They might also lose social status, have trouble accessing employment or benefits, or face obstacles in being admitted to schools.

See Working Group member Steve Feldstein's paper for more information and recommendations on **State Surveillance and Implications for Children**

2. Poor protection of children's sensitive data paves the way for even more surveillance and use in unanticipated and harmful ways



In a drive for efficiency, effectiveness and scale, children's data is widely collected for reasons of protection, health care, education, humanitarian aid, development assistance, and other social welfare purposes. Technology can improve efficiency and scalability of these services while data-improved tracking capabilities can contribute to better decision-making and targeting of funds and programmes. However, if internationally agreed norms and standards such as data minimization, purpose limitation, and privacy protection are not applied, children's confidential data are left unprotected from use or sharing in unforeseen, unanticipated, and harmful ways.[38] Furthermore, social service agencies frequently rely on technology platforms and tools developed by private companies. This blurs the lines between public service and commerce, and opens the door to monetization and commercialization of data.

Children's health data is one area where there are significant ethical and safety concerns. These were amplified with the arrival of the COVID-19 pandemic in 2020. As greater amounts of data are being collected in efforts to halt the spread of the virus, the traditional controls on health data sharing and use were relaxed by many governments.[39,40] Health data are generally considered sensitive and afforded higher levels of protection because they provide comprehensive information on an individual. Stigma and discrimination can result from poor protection of sensitive health data, especially in the case of HIV, STDs, and mental health conditions. While this affects people of all ages, the vulnerability and developmental stage of children means that this could have more permanent or long-lasting effects. Insurance companies might charge higher insurance premiums or deny coverage if they have information about past health conditions, and educators might make assumptions about a child's ability to learn or perform in school, based on sensitive health data.[41]

The advances made in technology and the potential for highly lucrative uses of health data have pushed the boundaries of privacy. Health data for research purposes used to be collected primarily through clinical research and regulated by ethics bureaux or institutional review boards. Health records for patient care were

largely held by local or national facilities offline. Today, unregulated digital health and well-being apps collect and process children's health data and combine clinical and consumer data for research purposes. Fitness trackers and wearables, menstruation tracking apps, and mental health apps are just some examples of private sector health apps popular among children and youth that collect highly sensitive data, including real-time GPS data and reported or inferred emotional states. Because mobile phone apps routinely collect so much identifying data, it becomes nearly impossible to de-identify data in order to protect privacy.[42] Even if consent for research is obtained, researchers often struggle to explain with accuracy and confidence exactly where data might end up, how long it is stored, how it is used, and by whom.[43] Children and youth might not understand that private and personal insights are being gleaned from their data and used for other purposes, such as marketing, influencing beliefs and behaviour, automated decisions related to services like health insurance, predictive analytics which may result in false positives or negatives, and various forms of background checks.

The use of technology in education systems is another area of major growth for the commercial sector. While it is generally accepted that health data are sensitive, in the case of education data, there is less consensus, despite the fact that education technology (ed tech) increasingly permeates so many aspects of children's learning experiences. In its 2021 study of COVID-related school closures, UNICEF found that 90 per cent of education ministries worldwide used some form of ed tech to provide remote learning for an estimated 268 million children.[44]

Ed tech software may be used to support school administration, to enable virtual classrooms, or to monitor student behaviour. Data collected through this technology is used to predict outcomes for individual students and schools as well as for child protection and security through applications that block certain websites or flag students who are deemed to be at risk of engaging in what are considered negative behaviours.[45] Some ed tech tools facilitate personalised learning. Regardless of their function, these kinds of software always introduce risks for student privacy and may feel invasive and overbearing for children.


© UNICEF/UNI74447/Markisz

See Working Group member Lindsey Barrett's paper for more information and recommendations on **Governance of Student Data**

Key issues arising from the use of ed tech in schools include:

- Lack of understanding by children, their parents and educators, of how data flow from one source to another, where they end up and whether they are used by vendors and third parties for potentially exploitative purposes like advertising and marketing. This opacity is exacerbated when platforms are used in non-English speaking countries, yet information is only available in English. In Brazil, for example, use of the G-Suite education platform greatly increased during the COVID-19 pandemic, yet the privacy notice and explanatory videos[46,47] were only available in English, making them inaccessible to most users in the country.[48]

- Lack of scrutiny of ed tech offered to schools, often through aggressive marketing techniques. These tools are presented by vendors as revolutionary and transformational and are often offered free of cost to under-resourced schools or communities. The resulting enthusiasm for ed tech may lower requirements for strict privacy standards.

- Lack of rigorous evaluation of a myriad of ed tech applications for their pedagogical efficacy. In the absence of assessment standards or sufficient guidance, the responsibility for evaluating a service's pedagogical value, as well as the safety and privacy risks it could impose, is left to individual schools.[49]

Tracking practices raise concerns about student privacy and the normalization of invasive tracking from an early age.[50] When adults feel constantly watched, they lose their freedom of expression,[51] and this is likely to be true for children too, in addition to losing space for play and experimentation. Commercialization through digital technology of both health and education spaces creates a worrying precedent for surveillance and the erosion of non-commercial space.[52]

Development and humanitarian organizations may unintentionally introduce harm while trying to help beneficiaries of their projects. As they digitize their operations and services, they create and capture more data about and from children. An infant provided with a wearable tracker as part of a nutrition programme, for example, will generate much more sensitive real-time data than they would if nutrition data were tracked on paper by a volunteer on a weekly basis.[53] If biometric data (which are body measurements related to human characteristics such as fingerprints, or DNA) is collected on children in a humanitarian setting as part of a beneficiary registration programme, the tracking and tracing of their movements becomes a

part of their daily existence. While this data can help agencies target their services and allocate budgets more efficiently thus allowing them to reach more children, its collection and use exposes children to higher levels of surveillance by state and corporate actors.[54]

The complexity of the data ecosystem leaves agencies struggling to gain meaningful and informed consent from children or their guardians when they digitize their services. While many organizations are starting to comply with GDPR, innovation and development tech applications are happening faster than the ability of many in the social sector to keep up, in terms of developing standards and protocols for their use. Smaller agencies may not be able to effectively address the complex issues of data governance, including special protections for children, due to lack of capacity and resources.[55]

Children and their data in a refugee setting

Children account for approximately 40 per cent, or 30–34 million, of the world's 79.5 million forcibly displaced population.[56] Forcibly displaced children, including refugees, asylum seekers, and internally displaced persons, are made increasingly vulnerable by systems that fail to protect and safeguard their data and rights. Surveillance and biometrics data collection could add additional strain on these children and contribute to their marginalisation. There are currently little to no effective protection mechanisms to safeguard forcibly displaced children's data across jurisdictions. According to the European Union Agency for Fundamental Rights (FRA), IT systems used by the EU that were initially created for asylum and migration management are increasingly being used for internal security purposes.[57] A revised proposal for the European Asylum Dactyloscopy Database (EURODAC) aims to lower the minimum age of a data subject to 6 from 14 and enable the collection of their biometric data (beyond fingerprints and facial image).[58]

The United States Department of Homeland Security has proposed the expansion of biometric data collection and use by US Citizenship and Immigration Services, including the collection of biometrics at any age.[59] Especially vulnerable children and their guardians are unable to meaningfully consent to the collection and use of their data as refusal to do so would limit their access to asylum or essential services, such as education, shelter or housing, food, livelihoods, among others. The experiences of forcibly displaced persons reveal a two-tiered system of data protection, whereby data protection laws and policies apply to those afforded citizenship within a jurisdiction, while those without citizenship are subject to data protection exemptions in the name of security.

3. Predictive analytics may amplify existing discrimination and bias

Artificial intelligence (AI) systems and different techniques they apply (machine learning, predicative analytics and others) are changing how many institutions work. These systems can analyse huge amounts of data quickly and at vast scale, finding patterns in data and using them to predict behaviours and automate decisions. AI is poised to bring an estimated US$13 trillion in economic outputs by the year 2030.[60]

What is algorithmic bias?

Algorithmic bias is the systemic under- or over-prediction of probabilities for a specific population,[61] for example, for children from a particular class, race, ethnic group, geographical location, or combination of some of the above traits and others. Causes of algorithmic bias include unrepresentative data, flawed or biased training data, context blindness, and the uninformed use of outcomes without human involvement in decision-making.[62]

Governments use AI systems to make decisions about asylum and immigration status, allocate benefits, and determine eligibility for parole. Social and traditional media apps and websites rely on machine-learning algorithms to curate content, predict behaviour and generate personalized advertisements. In the medical sphere, AI is used to model the spread of pandemics like Ebola and COVID-19[63] and to support vaccine development.[64] Some humanitarian organizations are exploring the use of AI in their operations in an effort to improve efficiency and to harness data, for example to predict migration flows, civil unrest, conflicts and climate disasters in order to be prepared to respond more quickly.[65]

One of the greatest concerns with AI systems and children is their reliance on modelling to make determinations that affect children's futures.[66] Algorithms tend to reproduce patterns of bias and historical discrimination found in the data used to train them. The use of machine learning tools to assess student performance has resulted in already marginalized children being further targeted for disciplinary actions and labelled pre-emptively as more likely to engage in criminal or other anti-social behaviours.[67] Scores used in criminal risk assessments in the United States have habitually recommended harsher sentences, higher bonds, and lower likelihoods of parole for black people, including black children and youth, than for white people despite these practices proving to be both unfair and unjustified in comparative studies of actual recidivism.[68] Bias and mistakes that lead to the exclusion of children or their families from cash transfers, scholarships, housing, health benefits or other aid and entitlements can have dire consequences.[69]

See UNICEF's **Policy Guidance on AI for Children** for more information and recommendations

There is no shortage of discussion on the ethics of AI systems – over 160 sets of AI principles have been developed since 2016.[70] The UN Committee on Digital Cooperation has warned against opaque algorithms where the underlying data and decision-making processes

cannot be examined, and UNICEF has called for explainable algorithms for children.[71] There is, however, very little legislation, and virtually no specific acknowledgement in national AI policies of how AI affects children.[72,73] Children often have less capacity than adults to identify instances of bias or discrimination in automated systems or to advocate for redress in such situations, yet as AI systems become increasingly common, their impact on children's lives and futures will only grow. As one scholar noted, the use of AI and machine learning are not only about privacy – our ability to control information about ourselves – but they are about our 'personhood' and our fundamental agency as human beings.[74]

4. Children's data may be used to manipulate and influence their behaviour

The same kinds of sophisticated behavioural science and data analytics that companies use to push children to consume products and media are sometimes used to influence children's other behaviours and beliefs.[76] Through constant capturing of children's data, digital services have developed comprehensive profiles on children, including their online actions, interests and behaviours. This allows for the development of algorithms that predict the types of content that will keep children engaged in scrolling, clicking, and watching digital content.[77]

Some social sector organizations and governments have adopted market segmentation and microtargeting, designed to maximize consumption and purchasing of products, to encourage or 'nudge' children to adopt specific beliefs about gender, political participation and other issues, or to encourage positive behaviours such as handwashing or using condoms.[78]

These techniques may also be used by groups with harmful goals such as pushing youth towards joining extremist organizations or spreading conspiracy theories and disinformation.[79] By manipulating amplification metrics on social media platforms these groups ensure that their content gains traction.[80] This content appears alongside editorial material that individuals trust, blurring the lines of what is true and what is not. These techniques have been credited with influencing elections in Brazil, India, the Philippines and the United States, for example, and for stoking violence and genocide in Myanmar.[81] Given that children's cognitive capacities and ability to discern true from false information is still developing, such techniques could be especially detrimental for the development of their critical and analytical thinking skills.

What is microtargeting?

describes a broad group of advertising techniques that rely on demographic and target-specific data – what people like, who they're connected to, what their demographics are, what they've purchased, and more – to segment them both as individuals and as small groups in order to then target them with specific online content. This technique can help deliver content that is interesting and helpful, such as recommendations that connect businesses to future customers and people to products and services they were searching for. It can also be exploitative and corrosive. Microtargeting can be used to flood individuals and groups with information that is inaccurate or biased and meant to sway, manipulate, or nudge their thoughts, behaviours and actions.[75]

Tracking children and using their data to influence them in harmful ways is problematic as it affects their freedom and agency. Opaque algorithms and non-transparent nudge techniques limit diversity of experiences and developmental opportunities for children. The resulting echo chambers[82] affect children's abilities to make independent choices and to access high quality, credible information.[83]

5. Legal frameworks generally overlook the risks for children of group data profiling

See Working Group member Andrew Young's paper for more information and recommendations on **Responsible Group Data for Children**

Data responsibility, privacy literature, and the policy ecosystem largely focus on individual data and have often overlooked or understated the risks in group data. With very few exceptions,[84] existing legislation aims to regulate the relationship between an individual, an entity that makes decisions about how to capture and process data, and an entity that processes the data. While important, this focus on personal data ignores that the data economy is increasingly driven not by the value of an individual's data, but by an accrued value that comes from combining multiple individual data sources and points with broader, group-level assumptions, often using machine learning.[85] Focusing only on individual data rights hides and exacerbates the risks that groups face. The challenges group data pose are immense and generally poorly understood, particularly the unique and amplified risks that children face.[86]

Common group-level classifications include:

- Demographic traits (e.g. ethnic background, disability or gender);[87]
- Associations (e.g. members of a certain religion or political party);
- A shared geo-location (e.g. people gathering in the same location);
- A common threat of harm or a similar type of vulnerability (e.g. specific ethnic or religious groups in a humanitarian setting); and
- Similar media consumption behaviours, buying habits, financial status and so on.[88]

What is the mosaic effect?

The mosaic effect refers to the compilation of disparate, often publicly accessible, datasets to create new and potentially sensitive insights. In 2000, Latanya Sweeney found that 87 per cent of the US population could be uniquely identified with no more information than their zip code, gender, and date of birth, for example.

The risks stemming from group data include physical risks particularly in conflict zones or violence prone areas. For example, when a group of children are identified as being physically present in a particular location (a school or waiting for a school bus), they could become a target of an attack. There might be online risks too, such as being targeted with a particular kind of content or messaging. Additionally, there are risks of re-identification of individuals within a group, including the so-called 'mosaic effect' in which individuals can be re-identified when sets of anonymized data are combined.[89] Individuals in a group generally struggle to exert agency over how their data are treated within that group. When data on a group are used, shared, or exploited, it is difficult for people of any age to raise complaints or seek redress in the case of wrongdoing. This is even more difficult for children and subgroups of children due to the kinds of vulnerabilities we have mentioned throughout this paper.

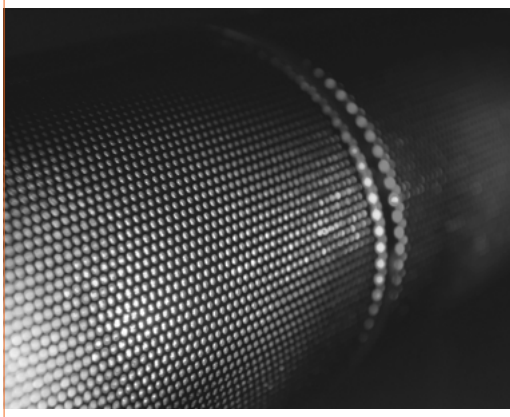
6. Achieving balance between different rights is challenging and requires careful consideration

Balancing children's rights to protection from conduct, contact, content, and contract risks[90] with their rights to access information, freedom of expression and the right to privacy creates ongoing tensions between rights that can be difficult to reconcile. Fundamental to a rights-based approach is an understanding that all rights are non-hierarchical, interdependent and indivisible.

See the paper by Working Group member Emma Day and colleagues for more information on **Encryption, Privacy and Children's Right to Protection from Harm**

Encryption is a crucial privacy-enhancing technology that encodes information so that it can only be read by certain people. 'End-to-end' is a robust form of encryption where in principle only those engaged in direct communication can access its contents. The secure communications that encryption enables protect the safety, privacy, and free expression of children and adults alike. Yet in some cases, encryption impedes efforts to monitor and remove child sexual abuse materials because it makes some kinds of communication more difficult for law enforcement to monitor. Encryption makes it difficult to deploy tools, such as Microsoft Photo DNA, that remove child sex abuse materials (CSAMs) and tools that identify offenders attempting to exploit children online.[91] This is a persistent tension, as tools that can work with end-to-end encryption and remove and disrupt CSAMs at scale, such as the use of advanced kinds of encryption together with an appropriately adapted tool, have not yet been fully developed.[92]

Due to these concerns, some children's organizations and governments are asking for legislation that would scale back end-to-end encryption. Privacy advocates tend to oppose this argument, as they fear that CSAM can be instrumentalized to open a door that leads to widespread government surveillance.



Age verification is another challenging area. The EU's Audiovisual Media Services Directive (AVMSD) requires children to be protected from online programs that "might seriously impair" the development of minors – such as pornography or gratuitous violence – through the use of "PIN codes or other, more sophisticated age verification systems". [93] The UK Age Appropriate Design Code also recommends the use of age verification tools or other age assurance methods to protect children from excessive data collection in online spaces designed for adults.

There are many ways to verify children's age online, yet the most common practice is for children to simply declare their age, without any proof. People are required to verify their age and identity before gambling online in some countries. Some propose that this requirement should be extended to commercial pornography websites,[94] age-regulated games, and social media platforms.[95] Age verification and assurance tools range from those that require the child to submit formal identity documents, to those that rely on parental identification, to those that estimate the age of the child through behavioural analytics or facial scans.[96] Many of these tools raise privacy and security concerns for both children and adults, regardless of whether the data is collected and controlled by the private sector or linked to government databases. This type of privacy infringement can only be justified where it is proportionate to the potential harm. Open questions remain about the degree to which parents should be left to oversee their children's internet use and the kinds of content that are harmful enough to children to warrant government regulation.

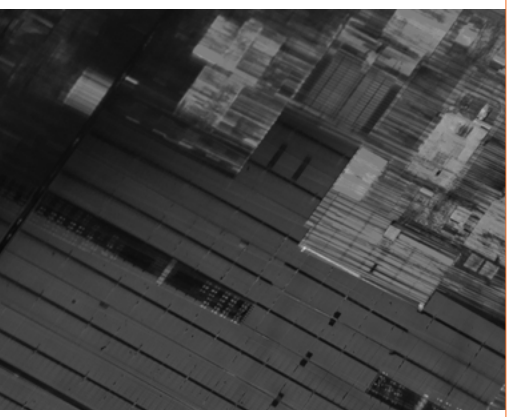
Parental controls include device settings that only allow children to download age-appropriate apps and games, filters that block age-inappropriate web content, and password controls that disable in-app purchasing to prevent large bills being run up at parents' expense.[97] These kinds of controls can be effective and important, especially for younger children. Other apps invite parents (and in many cases, teachers) to use more invasive types of surveillance to monitor children, including location tracking, internet search logs, websites visited and time spent on each, and monitoring of calls and texts.[98] This raises ethical questions regarding the child's right to privacy

vis-à-vis their parents and teachers, especially as they get older. Moreover, the data collected and monitored by these applications on behalf of parents is collected and processed by the commercial entity that operates the app, and is often shared with third parties including online advertising and analytics services.[99] In the process of attempting to keep their children safe, parents may be putting their children's sensitive data – and thus their children – at risk.

Tensions between rights such as the examples given here are likely to continue to arise and must be addressed in a balanced and proportionate way.[100]

7. Data governance regimes do not account for children's evolving capacities and differential experiences

Based on their age, capacity, context, and life circumstances, children and adolescents have differing levels of awareness regarding what information is collected online and for what purposes. They are not uniform in terms of their understanding of privacy, the devices they use, the sites they visit, or their purposes for going online. Children, however, are often treated as a homogeneous group when it comes to data privacy laws and policies.

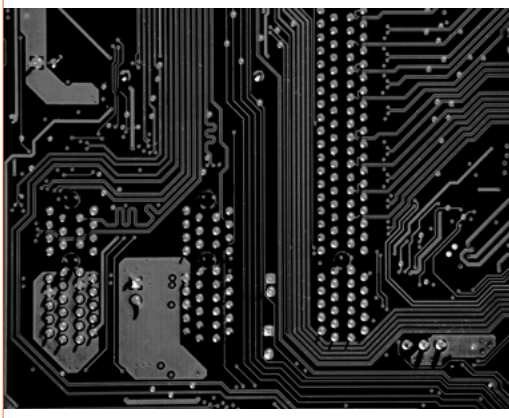


As children's competencies grow, their agency and capacities to exercise their rights also grow, and they require less direction. As individual children become better able to understand wider implications of data and privacy, they sometimes become better equipped to assess potential benefits and risks. However, children's evolving capacities are not linear, and children sometimes have particular vulnerabilities during adolescence that make them more susceptible to direct advertising that promises to enhance their social status. The Convention on the Rights of the Child allows for the recognition that children in different environments and cultures, and faced with diverse life experiences, will acquire competencies at different ages.[101]

Research shows that younger children tend to focus more on interpersonal privacy violations and less on corporate or government privacy violations. They are largely unaware that, when they use social media, they are sharing data beyond the information they post online, such as metadata, or data subsequently obtained by cookies.[102] Many children have internalized messaging from tech companies, governments and the media that individuals are responsible for their own privacy. While they are aware of online privacy issues, children

and young people often struggle to manage privacy settings.[103] A limited understanding of the nuances of privacy risks makes children more vulnerable to exploitation.[104] While their capacity and understanding may expand as they grow, there is no specific age at which children and youth are fully and automatically capable of managing their privacy, which is unsurprising given how much adults struggle to do the same. The Committee on the Rights of the Child has stated that the evolving capacities of the child should be seen as a positive and enabling process, and not as an excuse for authoritarian practices that restrict children's autonomy and self-expression.[105]

8. Most data regimes do not adequately address consent, child protection and representation



The legal bases that have been offered to children for collection of their data largely rely on consent. Consent is generally considered to be sufficient for the collection of data, even in the GDPR, which is widely considered the world's strongest data protection legislation. The Children's Online Privacy Protection Act (COPPA) sets the age of consent at 13 and GDPR at 16, as the age at which a child is judged to be capable of giving their *own* consent to the processing of their personal data online, although the GDPR allows States to elect to lower the age to 13.[106]

As discussed above, **age and capacity are often associated with children's ability to consent to their data being processed.** Children – often for clear and justifiable reasons – are subject to other people's consent and decision-making.[107] While this is a challenge in every context, in places where there is limited or low literacy, language skills, and bandwidth, consent becomes difficult, especially if parents and guardians are less digitally literate than their children.[108] The use of age as a representation of capacity, and whether children can understand terms and conditions and privacy policies that many adults cannot comprehend, may not be meaningful or appropriate. Consent by adults may also be a woefully insufficient guardrail of children's rights, given how much adults struggle to assess privacy risks, how many privacy decisions they confront per day, and how little useful information they're given to guide their decisions. Also of note is the sudden key event when the child receives the authority to control the data about themselves, often at age 13 or 16. This is a huge and sudden change in terms of both rights and responsibilities that a child ought to be well prepared for through the provision of comprehensive digital literacy education.

The age of consent and the ability to consent should be viewed separately from child-specific data protection. Children are entitled to special protection and consideration for their data until they reach the age of maturity (18) irrespective of the age of consent.[109] This protection extends to the right of rectification and erasure (often referred to as the right to be forgotten) and protection from profiling based on automated processing. The UK Age Appropriate Design Code offers this additional protection to all children, without changing the existing age of consent. Online service providers are directed to apply the Code's protections in a way that reflects the age range of their audience and the different needs of children at different ages and stages of development.[110]

See Working Group member Sean Martin McDonald's paper for more information and recommendations on **A Fiduciary Approach to Child Data Governance**

Narrow interpretations that limit children's data protection to mean 'consent for data processing' frees States, companies, and other organizations from responsibility for detrimental use of personal data and privacy violations. There is a power imbalance between data collectors' push to capture greater amounts of data and the capacity of families and children to protect themselves in an increasingly complex digital world.

While levels of agency differ between children of different ages, backgrounds and circumstances, their relatively limited agency in this complex digital ecosystem is disempowering. This is not a new issue. Almost every legal tradition considers the creation of credible representatives or 'fiduciaries' for vulnerable, ineligible, or incapacitated populations when dealing with decisions that affect their rights. Both the CRC and the United Nations Declaration of Human Rights establish that childhood is "entitled to special assistance".[111] Children need to be provided with solutions that amplify their voices and enable meaningful representation and engagement with regard to their data rights. This representation can take different forms, as we discuss in the next section.

© UNICEF/UN051301/Herwig

PART 2

Data governance regimes and how they apply to children

What does data governance mean in practice?

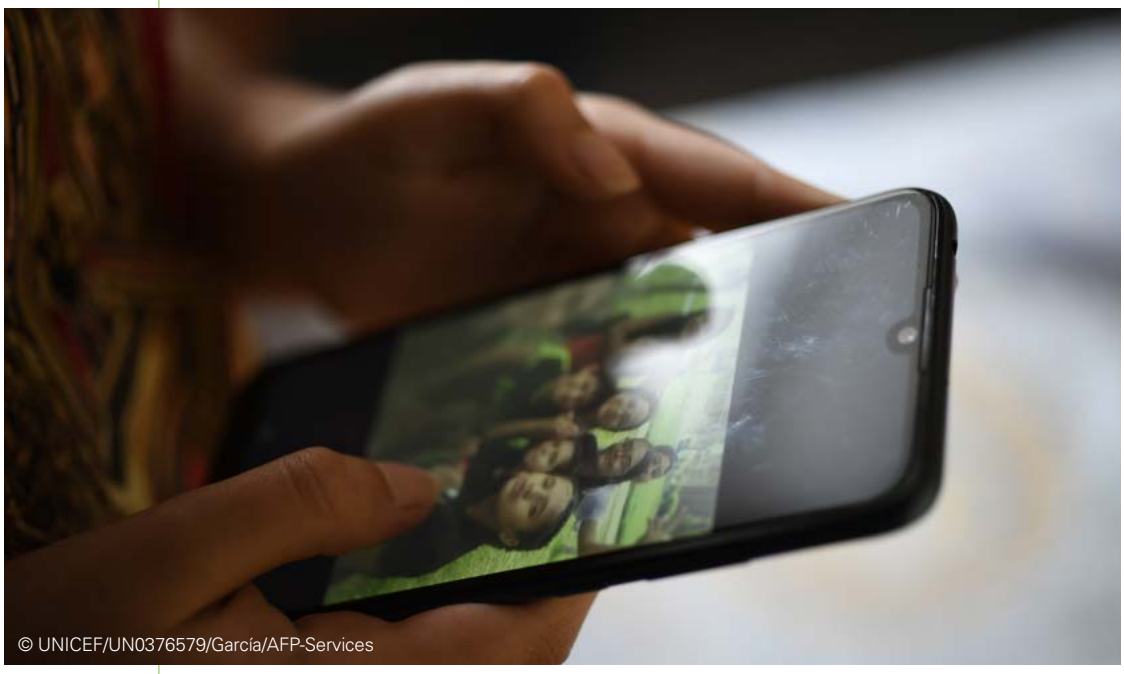
Data governance is a critical part of effective and safe management, use, analysis and communication of data. It includes aspects such as:

- Determining responsibility for data, datasets and databases;
- Development and enforcement of policies, roles, responsibilities and procedures;
- Establishing clear procedures and practices for how data can and will be shared internally and externally;
- Rules and expectations related to data privacy and security; and
- Setting accountability mechanisms for ensuring that policies and procedures are followed and respected, and resolving disputes arising from violated data rights.

Good data governance supports individual and group privacy rights, and also helps to generate improved collaboration and safe use of data within and among organizations and institutions.[112]

Data protection and privacy laws exist at global, regional and national levels, and all impact on children's rights. The degree to which these laws are implemented depends, amongst other things, on the strength of the rule of law in different parts of the world, the degree to which data subjects are informed of their rights and can access justice, and the jurisdiction over the technology companies in question. The development of data governance regimes is driven by the primacy given to the data economy and geopolitics, which are a battleground for data regulatory standard-setting and dominance in cyberspace. These geopolitical trends are currently playing out between the dominant global market forces of China, Europe, the United States, and a small number of multinational technology companies which sometimes take on a governance role themselves.

The political economy of children's data offers a wide set of considerations. Data cannot be de-linked from power and institutions, and data governance mechanisms should be careful to avoid digital data being used to cement power and profits for the privileged.[113,114] A key reason why an international data governance regime for children is needed, is to ensure that one nation or region's governance framework does not dominate the globe due to disproportionate economic and political power. Rather, children's data should be subject to an international legal and policy regime applying international human rights and child rights laws and norms that have already been widely negotiated and adopted around the world.



© UNICEF/UN0376579/García/AFP-Services

At the global level there is no comprehensive data governance legal framework, leaving a significant gap in governance in the digital age for both adults and children.

Existing governance frameworks

Existing international standards cover some elements of privacy and data protection rights, but these are fragmented across various international human rights treaties. Privacy rights that relate to children can be found in the Convention on the Rights of the Child and its General Comment No. 25, the Universal Declaration on Human Rights, the International Covenant on Civil and Political Rights, the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the Council of Europe's Convention 108+ which has a global reach beyond Europe. In addition, the Council of Europe Guidelines to respect, protect and fulfil the rights of the child in the digital environment require States Parties to limit the processing of children's personal data for commercial purposes.


© UNICEF/UN0352690/Vas

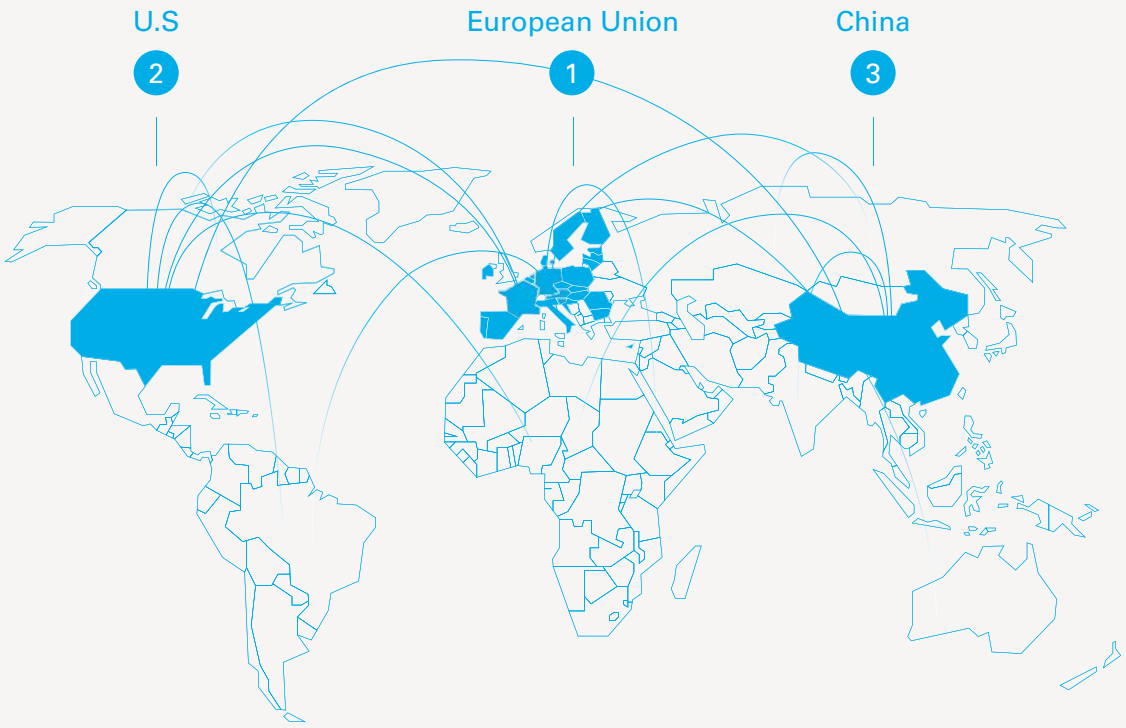
The Guidelines also raise concerns regarding the profiling of children, and recommend to prohibit profiling unless allowed by law and in the best interests of the child. Additional Council of Europe Guidelines on children's data protection in an education setting were adopted by 55 countries in 2020.[115] International human rights treaties are generally not binding upon their parties except in jurisdictions in which they are directly applicable, so in most countries their implementation is contingent on their translation into national law. In addition, the UN Guiding Principles on Business and Human Rights set out the corporate responsibility for human rights. Companies can assess how well they are meeting these responsibilities to children, in particular by carrying out a child rights impact assessment (CRIA), which should include aspects related to data collection and privacy.[116] The General Comment No. 25 also requires States to promote the use of CRIAs by businesses relating to the digital environment.

Committee on the Rights of the Child General Comment No. 25

In March 2021 the Committee on the Rights of the Child released General Comment No. 25 on children's rights in relation to the digital environment. For the first time the Committee elaborates on the application of the CRC to aspects of children's privacy and protection of their data. General Comment No. 25 calls for States to:

- Prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of their actual or inferred characteristics, including group or collective data;
- Ensure that agencies with oversight powers relevant to children's rights, such as data protection, investigate complaints and provide adequate remedies for violations or abuses of children's rights;
- Design age-based or content-based systems to protect children from age-inappropriate content, in a manner consistent with the principle of data minimization;
- Balance content moderation and content controls with the right to protection against violations of children's other rights, notably their rights to freedom of expression and privacy; and
- Respect the child's right to privacy in automated processing of children's data and in digital surveillance, which should not be conducted routinely, indiscriminately or without the child's knowledge or, in the case of very young children, that of their parent or caregiver.

FIGURE 2 DATA GOVERNANCE LAWS FROM EUROPE, THE US, AND CHINA ARE THE MOST INFLUENTIAL ACROSS THE WORLD



1 **At the regional level,** the EU's General Data Protection Regulation (GDPR)[117] currently appears to have the greatest global influence on national data protection laws around the world.[118] It provides high level data protection for both adults and children, with special protections in place for children, and rights attaching to the individual child rather than to the purpose for which the data are being collected. The GDPR allows States to set the age at which children's data can be collected without parental consent at between 13 and 16. In Europe, privacy and data protection are rights also enshrined in the EU Treaties[119] and in the EU Charter of Fundamental Rights.[120]

The GDPR applies to any data controller or processor with an establishment in the European Union, regardless of whether processing takes place in the EU. It also applies to controllers or processors not established in the EU, when they process the personal data of subjects who are in the EU, by offering them goods or services or by monitoring their behaviour within the EU. Consequently, a number of businesses around the world have started using geo-location technologies to block users accessing their services from the EU, rather than extending data protection rights to them.

The GDPR sets a standard whereby data is governed by its function, rather than according to who is collecting the data. In Europe private companies are generally regulated under commercial law which prioritizes commercial interests, whereas governments are held accountable under public law which prioritizes individual and collective human rights.[121] In the United States, consumer protection laws are intended to protect the needs of individuals as consumers in the marketplace (but not as individual rights holders) without unduly limiting the ability of businesses to discover new ideas or profit from them.[122] Given the preponderance of public-private partnerships (PPPs) that collect data from children and share it between them, governing data according to its function, rather than according to the act of collecting the data, provides a unified approach to the rights of a child as a data subject alongside the different legal frameworks that may apply to the public or private sector entities involved in the PPP.

In 2014 the African Union (AU) Convention on Cyber Security and Personal Data Protection was passed, which provides general data protection provisions for the whole Continent. The AU Convention only refers to children in the context of child sex abuse materials (referred to in the text as 'child pornography') and does not give them any extra rights to data protection different to adults.[123] At the time of writing of this Manifesto, the AU Convention has only been ratified by 8 out of 55 countries in the AU.[124] In a 2020 artificial intelligence needs assessment survey across Africa, UNESCO found that personal data protection and data governance was an urgent and important area of work in 23 countries in the region (71 per cent of those surveyed).[125]

The Asia Pacific Economic Cooperation (APEC) Privacy Framework has led to an increased focus on privacy legislation in the Asia Pacific region.[126] The APEC Privacy Framework advises that where an organization provides a mechanism for exercising choice in relation to data collection from children, the information should be conveyed in ways that are age appropriate.[127] Mandatory national data localization requirements are becoming a widely adopted approach to some of the cross-border legal challenges on the internet in the APEC region, but this leads to greater costs for both companies and consumers.[128] This is required by China and Indonesia, and is generally viewed favourably by countries in Asia including the Association of Southeast Asian Nations (ASEAN) where there is a perception that the State's ability to enforce their laws is being undermined by foreign companies and interests.[129]

At the national level, data protection laws are becoming more common across all regions. In 2020, 128 jurisdictions had data protection laws in place.[130] It is likely that by 2030 close to every country in the world will have a data protection framework, in part to allow for data flows in accordance with bilateral and regional trade deals.[131] In terms of market power, China and the US are said to be the global controllers of data, creating 'data-opolies' through their market dominance.[132] Some of the leading apps used by children around the world come from these two countries, including Facebook and Google from the US, and TikTok and games owned by the Epic group of companies in China. This makes the data protection laws from China and the US particularly significant to children worldwide.

2 **The United States** has one of the few federal laws directed specifically at protecting children's data privacy: the Children's Online Privacy Protection Act (COPPA) covers only commercial entities but also offers some protections for children in schools.[133] Although the age at which children can consent to their data being collected under COPPA is 13, which is lower than the recommended 16 under the GDPR, more guidance is given by COPPA regarding satisfactory methods to obtain consent from their parents.[134] Historically the US has had a lax approach to the use of personal data, but the international legal environment now appears to be changing, putting the US under increasing pressure to meet common global standards.[135] The California Consumer Privacy Act (CCPA), contains increased data privacy protections for children and provides for those aged 13 to 16 to be able to opt in to collection of their data. Unlike adults however, they cannot be presumed to opt in with the only option available being to opt out. This enhanced protection for 13- to 16-year-olds under the CCPA could have the effect of raising the standard across the whole of the US, depending on the compliance incentives that the law's enforcers create.

UK Age Appropriate Design Code: A code of practice for online services

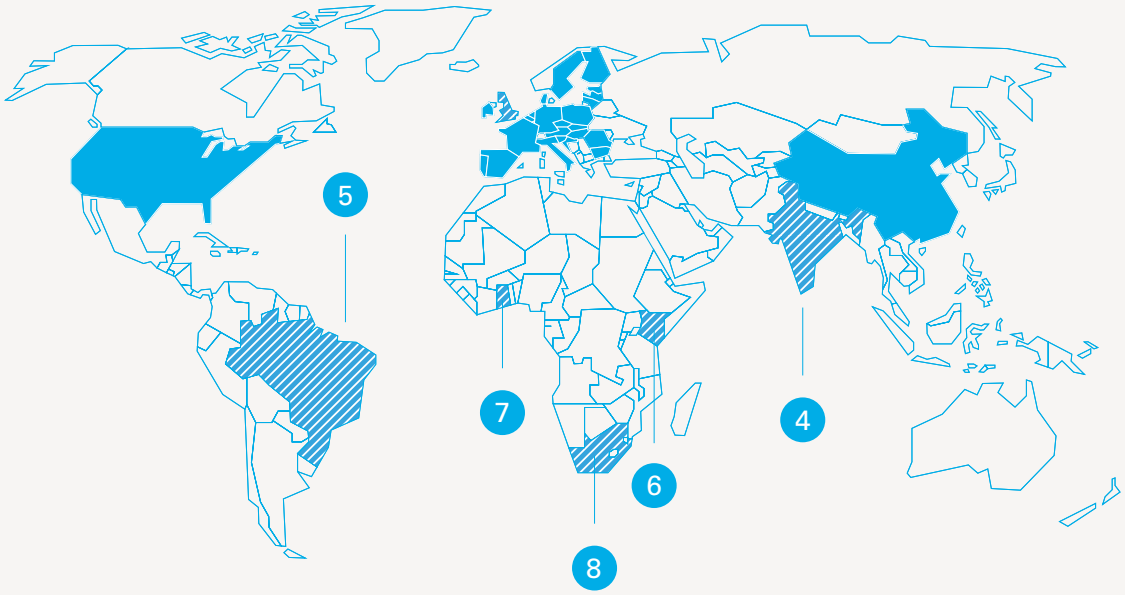
The UK's Information Commissioner's Office (ICO) has produced the Age Appropriate Design Code (AADC) which applies to online information society services including apps, programs, connected toys and devices, search engines, social media platforms, streaming services, online games, news or educational websites and websites offering other goods or services to users over the internet. The new age-appropriate code requires companies to provide default settings which ensure that children can have maximum access to online services whilst minimizing data collection and use by default.[136] One of its key objectives is to help companies comply with the GDPR. Companies will have to demonstrate that they are complying with the AADC, otherwise they potentially face being fined. The AADC is grounded in the CRC and reflects a risk-based and proportionate approach, calling for companies to:

- Create an open, transparent, and protected place for children online;
- Follow a set of standards for design and development of online services likely to be accessed by children;
- Consider the best interests of the child when processing their personal data;
- Implement high privacy settings by default; and
- Use language that is clear and easy for children at different development stages to understand.[137]

3 **China** has recently implemented several new laws that now cover data protection in relation to most of the private sector, including the E-Commerce Law of 2018,[138] and the 2019 Regulation on Cyber Protection of Children's Personal Information. The 2019 Regulation is aimed at websites and applications which may potentially have underage users, such as gaming platforms, e-commerce sites and social media platforms. Although federal laws currently only protect children up to the age of 14, this has extra-territorial effect which means that it applies to any company collecting data from children in China, even if the company is based outside the country.[139] In China, data protection laws provide children with data rights vis-à-vis the private sector, but not vis-à-vis the State.

Other **middle-income countries** are home to large proportions of the world's children, and as such are of particular interest to developers of apps and games for children, which makes their data governance frameworks an important part of the global landscape. In 4 **India**, for example, Chapter V of the Personal Data Protection Bill 2018 contains special protections for children. The draft Bill requires anyone collecting data from children under 18 to do so while complying with the "best interests of the child" standard. Data collectors are also reportedly prohibited from profiling or tracking children, and are not allowed to target advertisements directly to children.[140] In 2012 the Indian Supreme Court held that "Children around the world create perpetual digital footprints on social network websites […]. They should not be subjected to the consequences of their childish mistakes and naivety, their entire life", seemingly providing for a right to be forgotten.[141] A second draft of the Bill is currently before the Indian parliament awaiting approval.[142]

FIGURE 3 EMERGING DATA PROTECTION LAWS FROM SEVERAL MIDDLE INCOME COUNTRIES ARE AN IMPORTANT PART OF THE GLOBAL DATA GOVERNANCE LANDSCAPE FOR CHILDREN



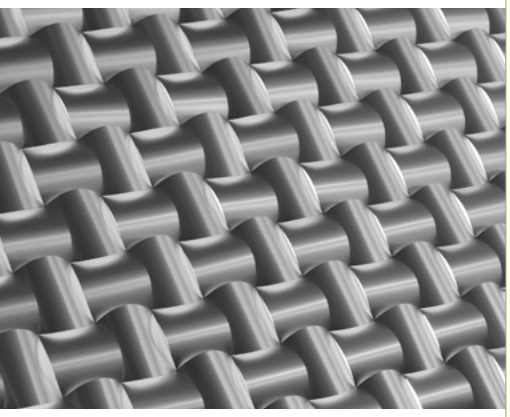
5 **Brazil's** new data protection law, which came into effect in August 2020, contains increased data privacy protections for children. It requires companies to be transparent about the data they intend to collect and the purposes they will be used for. Data controllers are also required to make reasonable efforts to obtain consent from children's parents and are not allowed to make children's use of games or apps conditional on their disclosure of personal information.[143]

Although there appear to have been a proliferation of new general data protection laws in low-income countries in recent years, few of these include extensive specific protections for children's data. There have been some recent promising developments however, such as 6 **Kenya,** which enacted a Data Protection law in 2019 specifically prohibiting data collection from children without parental consent, and 7 **Ghana,** which defines children's data as sensitive under its Data Protection Act 2012. Rwanda's Child Online Protection Policy recommends the strengthening and realignment of domestic legal and regulatory regimes related to online protection for children, and specifically recommends introducing data protection regulations to ensure children's data are protected appropriately, and collected only where necessary, with high levels of security and care. 8 **South Africa's** Protection of Private Information Act mandates responsible parties to obtain consent from a 'competent person' before processing children's personal information with a few prescribed exceptions.[144]

The lack of comprehensive attention to children's data rights in low-income countries could arise for a number of reasons, including a general lack of government prioritization of data protection as well as a lack of public interest in this issue,[145] or in child rights in general, or a lack of public trust in their government's ability to protect children's interests. Children's public services and the rule of law also tend to be weaker in countries with fewer resources, which means that children's rights are less likely to be prioritized and integrated into data protection legislation.

In several countries, aspects of data governance have been devolved to State or local levels via subnational data protection authorities, and in some countries local leaders are organizing themselves to take control of their own data. In Helsinki and Amsterdam, for example, public AI registers have been developed to ensure meaningful transparency so that information about AI systems in use in the city (which are essentially data systems) is publicly available.[146] This kind of devolution of governance of children's data could allow for increased participation of children and their parents at a local level.

In the context of self-regulation, currently large multinational technology companies have the power to make unilateral decisions regarding data governance for children.



Private sector de facto governance

Those governments that do have influence are mainly those from the most powerful markets: China, the EU, and US. This leaves children in the Global South particularly at risk of data exploitation by private companies in the face of which their governments are rendered essentially powerless. Protection against the use of commercial data for state surveillance of children is also compromised when this is left purely as a matter of national security at the total discretion of each government. Vast amounts of data have been collected from children and are now concentrated in the control of around 5 to 10 multinational companies based in the US and China.[147] However, there is a sector-wide lack of transparency related to the collection and processing of data, and this applies to children as much as to adults. The Ranking Digital Rights Corporate Accountability Index found in 2019 that most companies fail to disclose important aspects of how they handle and secure personal data.[148]

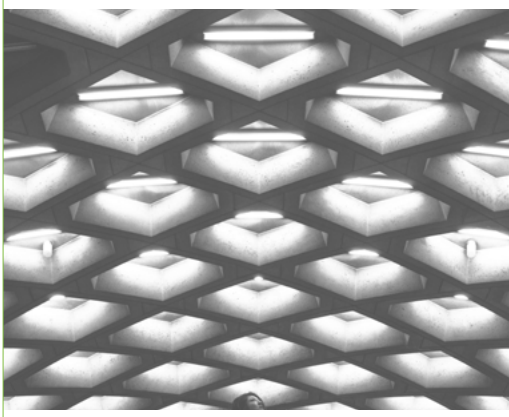
The persistence of an inconsistent landscape related to data governance for children can lead to 'forum shopping' by private companies, which then locate themselves in jurisdictions that require less stringent data and privacy protections for children. For example, the UK Information Commissioner discovered during the course of an investigation into Cambridge Analytica that the company was considering moving to the Caribbean or to another country where it could be outside the scrutiny of a regulator.[149]

As the late European Data Protection Supervisor, Giovanni Buttarelli, commented in his manifesto, Privacy 2030: A Vision for Europe, "increasingly private platforms intermediate the relationship between citizen and State. Data defines individuals and determines how they can be treated. The terms of service therefore become, in effect the law."[150] A study of more than one million apps on Google Play Store conducted in 2019 found that none of the Google app stores engaged in a comprehensive and systematic review of the privacy policies of the apps they were hosting,[151] and it is likely that this is also true for other major app stores due to the lack of any specific legal requirement for them to carry out this kind of audit, and the lack of other sufficient incentives for them to police their marketplaces more carefully.

As governments increasingly rely on public-private partnerships to carry out key functions in the areas of education, health and social welfare, public officials are often not privy to key data points that could inform public policy and even prevent security risks to children.[152] Governance by democratically elected leaders is fundamental to the rule of law, but when the private sector holds large amounts of data, governments are disempowered and there is a shift towards de facto governance by the private sector.


© UNICEF/UN0403705/Raab

Parents' or schools' 'governance' of children's data use



In the case of children and childhood data, an additional layer of governance comes into play with respect to caregivers' and educators' data management activity on behalf of the child. Because in most jurisdictions children are not able to consent to their own data collection before the age of 13 (or 16 in some cases), companies, governments or organizations must seek consent from the parent or caregiver where consent is required to collect data from younger children. As with children, parents and caregivers vary greatly in their digital literacy and in their capacity to engage with their children's use of technology. Some parents may not speak the dominant global languages used in the Terms and Conditions of the technology platforms used by their children, and even where they do they may not have the time to read them, or to understand the choices presented in relation to data collection from their children. The UK ICO advises companies to provide their privacy information in the language that their intended audience is most likely to understand.[153]

In the education context, often schools as public authorities will make decisions about data collection from children on their behalf, without any legal duty to consult with the children themselves or their parents. The Council of Europe Guidelines on Children's Data Protection in an Education Setting require schools to carry out a strict necessity and proportionality test before the collection of all personal data from children to ensure data minimization.[154] Any use of children's data should meet a child's reasonable expectations and meet the principles of purpose limitation and restrictions regarding storage and retention. For schools to be in a position to make necessity and proportionality assessments they must be given detailed guidelines by governments regarding the parameters in relation to data collection from children for education purposes, and the implementation of these guidelines must be overseen.

Data flows are a core component of today's digital economy, and children's data make up a large portion of this economy.

The data economy as a driver of good data governance for children

Businesses increasingly depend on advanced analytics based on high volumes of personal data for their fundamental operations, especially in the internet of things and artificial intelligence sectors which include ed tech, toys powered by AI, and immersive video games.[155] Interoperability and cross-border data flows are critical to every scale of this digital economy from national, to regional, to global, and harmonized laws are a prerequisite for each.[156]

Data regulations generally aim to balance elements of privacy protection for individuals, including children, with efforts to enable innovation and data flows to grow the digital economy to benefit individuals and businesses. However, this balance is difficult to establish. While some camps push for greater protection of personal data, privacy rights and security, others are more concerned about addressing barriers to digital trade and data flows.[157, 158] We argue that it is possible to establish frameworks that ensure privacy and data protection for children as well as openness to the mobility of data, and these kinds of frameworks can be a net benefit and a positive contributor to the development of the data economy.[159]

A simple economic lens is insufficient for viewing the data economy. The geopolitics of the digital economy results in larger markets such as the US and the EU competing for primacy of their legal approach and regulatory standards. In some ways, the European approach has taken precedence through implementation of the GDPR, because the EU has imposed data protection requirements on third countries wishing to trade data with the region. Other regions, such as China and the US, have imposed minimal prerequisites of their own to trade with their respective markets. Businesses can therefore trade with all three major markets simply by levelling up their data protection compliance to meet the standards laid out in the GDPR.

The current shortfall in data governance has been likened to the rapid and unregulated development of financial services globally in the 1990s and 2000s prior to the Great Recession when it was assumed that, in pursuit of a global good, self-interest and reputation would regulate the private sector's behaviour. One suggestion is to draw on lessons from the financial crisis, that resulted in the creation of the Financial Stability Board which was given a mandate by the G20 to promote the reform of international financial regulation and supervision. The Board also played a role in standard setting and promoting national implementation of the agreed international standards.[160] International internet governance initiatives started some time ago, with the OECD, UN and the Internet Governance Forum (IGF) proposing common rules.[161] The multi-stakeholder model, at the heart of IGF, and the UN Secretary General's High-Level Panel on Digital Cooperation, contrasts with the newly emerging models and proposals that favour data sovereignty or governance of data by a few global powers.

To address these challenges, some propose the establishment of a World Data Organization with status similar to the IMF or the World Bank to allow for data flows across nations.[162] While we strongly believe in the centrality of rights and primacy of international norms and standards, regardless of the future direction of data governance regimes, children's rights should be front and centre of the rule makers' minds. In addition, any multi-stakeholder model must include democratic and independent leadership that does not allow powerful government or commercial interests to dominate.

One of the key factors in assessing the strength of data privacy protection for children in any country is the existence of robust formal data protection laws.

Prerequisites for strong data protection for children: robust laws, effective implementation and absence of surveillance

The effectiveness of enforcement and the extent of surveillance are two other key dimensions that must also be taken into consideration.[163] Even where robust data privacy laws exist, they are not always properly implemented. In other cases, sometimes other laws take precedence, such as those that permit government surveillance for reasons of national security and to combat terrorism or during public health emergencies.

In many countries, primacy is given at a national level to provisions of specific laws related to national security over data protection laws and there is little opportunity for public review of this prioritization.[164] Article 23 of the GDPR, for example, allows for derogation from the rights protections foreseen on the grounds of national security, defence, public security and crime prevention, but any derogation must be necessary and proportionate for a democratic society. The Court of Justice of the European Union (CJEU) has recently played a role in ensuring that surveillance laws in both the US and parts of Europe are not allowed to override rights to data protection, and although these decisions do not relate specifically to children's data, they are equally important to their rights in the context of data governance.[165,166]

Strong national and subregional Data Protection Authorities (DPAs) oversee the effective implementation of data protection laws, especially where they work together across regions.[167] DPAs are independent public authorities that are responsible for supervising the application of data protection laws by carrying out investigations and imposing fines and other sanctions. They also provide expert advice on data protection issues and handle complaints from the public, including from children and their representatives, about breaches of data protection laws. DPAs have a recent history of collaborating across countries and regions to address data protection breaches by multinational companies. For example, in 2018 DPAs from Canada, Hong Kong and the US collaborated on an investigation into a connected-toy company, resulting in a Federal Trade Commission enforcement action against the connected-toy manufacturer for collecting children's data without parental consent.[168]

In order to be effective, DPAs must have the capacity to litigate, impose fines and other sanctions on lawbreakers, and a mandate to provide remedies to children whose rights have been breached.[169] At the Institute of Advanced Privacy Professionals Europe Data Protection Intensive in 2020, it was noted that children's privacy is becoming a hot topic for DPAs within the EU, especially in relation to verifying parental consent.[170] To assist those countries which do not currently have DPAs it is recommended that resources are allocated to establish one. Globally, the expertise within DPAs to address children's data governance issues must be supported and strengthened.

Non-profit organizations and think tanks also play a role in holding tech companies and governments accountable for implementing data protection laws, albeit in the face of immensely powerful legal teams within corporations and governments. It has been noted that corporate secrecy and intellectual property rights are more protected in practice in most countries than individual privacy and personal data.[171] There is a lack of transparency around the kinds of data being collected from children, and how this is being used and shared. This is partly because private companies have disproportionate resources available to enforce their own rights, compared to children and non-profit organizations acting on their behalf.

© UNICEF/UNI232328/Noorani

PART 3

The Manifesto: why we need an international approach to data governance for children

As all areas of children's lives become increasingly intertwined with digital technologies, it is possible to envision a future in which these technological advancements are primarily applied in service of children and their communities. With data having even bigger impacts on children's lives, we would like to see the benefits of such data collection and use spread evenly across the Global North and the Global South. But to achieve such a future for children where data is primarily used as a force for good, we need to grasp current opportunities to set the necessary guiderails and benchmarks which will help us govern children's data in a responsible way.

This Manifesto, therefore, calls for children's rights to be a specific and central element of all international, regional, and national legislation related to data governance. To ensure that children's data rights are protected equally across the globe, and to allow the growth of a digital economy that can benefit children, a consistent level of legal protection is required throughout the world. This is particularly important given children's vulnerabilities to abuses of their data, their capacity to consent as they move through different stages of childhood and the degree to which their lives are being impacted by data collection, sharing and processing.

This Manifesto does not seek to replace internationally agreed upon standards and principles, actions, and mechanisms for data governance, but rather looks to build on these, through good global data governance for children, and child-centred innovation in both policy and practice. Such an approach is needed for several reasons, including:

- Good data governance can facilitate a fair data economy, the cross-border nature of data flows and data storage practices, including children's data;
- The international approach is necessary to address geopolitical power imbalances: geopolitical (among states), geo-commercial (among companies) and those between a child and actors responsible for realisation of their rights, including the states and companies;
- It can enable harmonization of data protection rules across plural legal systems and different philosophies and contexts;
- It allows national data governance frameworks to be grounded in and legitimised by previously established international human and children's rights laws and institutions; and

- An improved data governance regime that is inclusive of children would also help to foster public trust, and especially trust by children, in the custodians of their data.

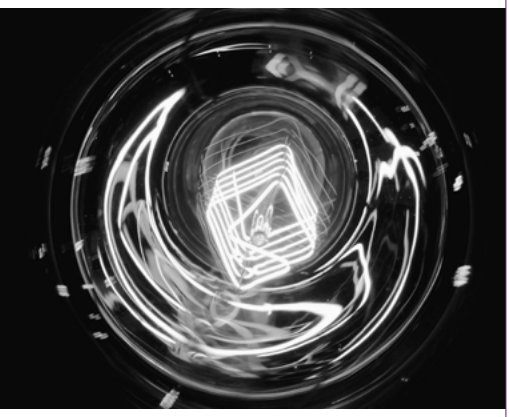
The foundation of a child-centred governance regime should be in previously established international human and children's rights laws and institutions, built upon by incorporating rights-based approaches to data governance from diverse regions around the world.

The CRC should be directly applied to the use of children's data, ensuring that they are not discriminated against, have the right to be heard, data are processed in their best interests, and according to their age and evolving capacity. Children's rights to freedom of expression, identity, assembly, privacy, and protection from exploitation must also be respected and promoted in the digital environment. The use of children's data should promote their rights to development, health, education, rest, and play.

Ensuring that the full spectrum of children's rights are upheld in relation to data governance means that the principle of data minimization must be prioritized. At the same time, we must ensure that data collection is not minimized to the point that groups of children are marginalized, for example because their data has not been included in data sets that are used to develop laws, policies and services.


© UNICEF/UNI43002/Mohan

Strengthening of norms, standards and principles



This Manifesto calls for the strengthening of norms, standards and principles specifically related to data governance for children, and their proactive implementation throughout the world. These should adhere to internationally agreed standards and principles of both data governance and children's rights. Amongst these standards the best interests of the child and the impact of data on their well-being and autonomy must be given the highest consideration. Further, data governance frameworks must be implemented with due regard to children's specific and unique identities, evolving capacities, and circumstances, beyond the bare minimum required by data protection laws.

1. **PROTECT** children and their rights through child-centred data governance.

Broad international and national data governance frameworks and those specifically addressing children need to build upon, rather than replace, already existing standards for data processing, such as the Responsible Data for Children (RD4C) Principles, the Institute of Electrical and Electronics Engineers (IEEE) Standards,[172] the UK Age Appropriate Design Code, the GDPR, and national child data protection laws as outlined above. In particular, the RD4C principles should be embedded in all data governance frameworks.

States should ensure that children's data protection and privacy regulations apply to all public services, including those services provided by the private sector or civil society organizations and other situations where companies have access to and use of children's data. Such regulations should also control children's data collection, use, sharing and storage by foreign companies within the State, and should be in place before the roll-out of new systems.

Responsible Data for Children (RD4C) Principles

The RD4C principles provide guidance, tools and leadership to support the responsible handling of data for and about children.

Participatory
Engaging and informing individuals and groups affected by the use of data for and about children.

Professionally accountable
Operationalizing responsible data practices and principles by establishing institutional processes, roles and responsibilities.

People-centric
Ensuring the needs and expectations of children, their caregivers and their communities are prioritized by actors handling data for and about them.

Prevention of harms across the data life cycle
Establishing end-to-end data responsibility by assessing risks during the collecting, storing, preparing, sharing, analyzing, and using stages of the data life cycle.

Proportional
Aligning the breadth of data collection and duration of data retention with the intended purpose.

Protective of children's rights
Recognizing the distinct rights and requirements for helping children develop to their full potential.

Purpose-driven
Identifying and specifying why the data is needed and how the intended or potential benefits relate to improving children's lives.

State and private sector surveillance of children should be controlled and minimized, recognizing the particular vulnerabilities of historically marginalized, underrepresented, and minority groups. Children's rights to peaceful assembly and association must be protected in the digital environment, free from state surveillance carried out by government authorities directly or in collaboration with private sector entities. There is a need to ensure accountability for state surveillance by authorizing independent judicial authorities to monitor against abuse and provide remediation as needed. There should be a presumption against surveillance of children with limited national security exceptions that are concrete, defined, and time-bound. Individual children should not be compelled to use surveillance applications, programs, or systems unless validated by legitimacy, necessity and proportionality tests.[173] Adherence to all norms

related to surveillance of children should be incorporated into the requirements for EU adequacy assessments and other similar cross-border data-sharing and trading agreements.

States should ensure that algorithms used in relation to children, such as safety and monitoring tools, health apps, and behavioural analytics tools are regulated and that profiling and nudging of children's behaviour is strictly minimized. States should mandate companies creating and using algorithms to provide a transparent explanation of the ways in which they make decisions, and about the data used to train such algorithms. The UN Committee on Digital Cooperation has recommended against opaque 'black box' systems, and UNICEF has called for explainable algorithms for children.

2. **PRIORITIZE** children's best interests in all decisions about children's data.

Recognizing the importance of using children's data to benefit their development and services, we believe that in all uses of children's data in the digital environment, the higher risk threshold needs to be established and their best interests should be a primary consideration. We hope this Manifesto encourages further deliberation of the best interests of the child in the context of data collection that resolves trade-offs between participation in data processing and minimization of risks. Some basic requirements are:

- **Governments and companies should ascertain the impact** on children of their data collection, processing and storage practices, in order to ensure that priority is given to children's rights.
- **Best interests need to have greater strength and validity** than any other established legal basis for data processing activities such as consent, performance of a contract, legal obligation, vital interests, or public task.[174]
- **Children's data should not be processed in ways that are shown to be detrimental** to them, such as persuasive design to extend engagement, marketing and behavioural advertising.[175]
- **In all products and services used by children it is important to:** limit biometrics collection; prevent the economic exploitation of children's vulnerability for marketing purposes; and to restrict profiling that could lead to behaviour modulation or discrimination.[176]

- **Data should not be used to power algorithms that interfere with children's rights** to autonomy and self-determination. The CRC General Comment 25 encourages States to define and prohibit digital practices that manipulate or interfere with children's right to freedom of thought and belief through emotional analytics or inference; and automated systems should not be used to affect or influence children's behaviour or emotions or to limit their opportunities or development.

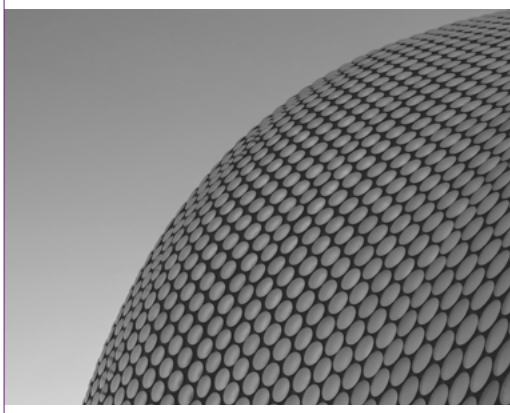
As digital economies further develop and expand, the international community must demand that States and companies address the commitments we have made to children's rights, and to their future under the Sustainable Development Goals. Platforms that create and administer digital rights for children, de facto take on a duty of care towards them which must be fulfilled to realize the fundamental rights of the child. This is the only way that big data, artificial intelligence and emerging technologies can be harnessed safely and responsibly for the public good and to further children's rights around the world.[177]

3. **CONSIDER** children's unique identities, evolving capacities and circumstances in data governance frameworks.

Global and national data governance regulations must be flexible enough to be applied in different contexts. We recognize that children around the world have unique identities, their capacities evolve throughout their childhood, and they live in extremely diverse circumstances with varying degrees of parental support. This means that data governance regulations must balance the need for legal certainty with the scope for them to be implemented in accordance with the diverse and evolving capacities of the child.

The UK Age Appropriate Design Code, the implementing guidance for the GDPR as it applies to information society services used by children in the UK, sets out five age ranges which correspond to theories related to child development in the UK. It serves as a guide to the capacity, skills and behaviours a child might be expected to display at each stage of their development. Those age ranges are:

- 0-5: pre-literate and early literacy
- 6-9: core primary school years



- 10-12: transition years
- 13-15: early teens
- 16-17: approaching adulthood

This kind of guidance is helpful to assess the risks posed by data collection and processing, and to assess the capacity of the child to understand and have an appropriate level of agency over their own data.

Respect for children's right to self-determination and data autonomy is critical and needs to be given due weight based on children's evolving capacities and progressive acquisition of autonomy. This would include children's right to data erasure and de-indexation when they reach adulthood particularly in those situations when the data was provided when a person was a child, without their full understanding of the implications of these actions.[178] There is a need for the private sector and public policy makers to work together to find ways for children to be given meaningful and accessible options to have their data erased, that are not too onerous for the child, and which do not require platforms to collect additional data related to their users' date of birth.

Notwithstanding guidance related to stages of childhood development, **all children are entitled to special protection and consideration** for their data until they reach the age of maturity (18), regardless of capacity to consent.

Marginalized groups of children should not be left behind in data governance frameworks. Algorithms can be biased against children whose characteristics differ from the data used to train the AI.[179] Data governance regulations should dictate the limits of the use of ed tech, health tech, and other kinds of AI that involve automated decision-making, to ensure that children whose characteristics are outside the norm are not marginalized and problematized by the AI. For example, AI algorithms used in schools to assess students' prior and ongoing learning can facilitate placement in appropriate subject levels. However, if the design of these algorithms does not take into account students' nuanced experiences, it may result in low income and minority students being trapped in low-achievement tracks with reduced expectations.[180] Further, data governance regulations must address the limits of the 'anonymization' of personal data, and the

potential harms that can be caused by group data for minority or marginalized groups of children.

Relatedly, there is a need for the regulation of data collected from children for the purposes of research, to ensure that children's rights to privacy are balanced with the need to ensure that groups of children are not underrepresented in research that might benefit them, particularly in medical or behaviour science.

For example, algorithms are increasingly being used for medical research, but most drug trials are carried out using data from males from white ancestries, whereas disease patterns, clinical presentation and the required treatment are known to be strongly influenced by gender, ethnicity, and socioeconomic status. This leads to a gap in the evidence regarding the efficacy or safety of drugs on females and those who are not white.[181]

© UNICEF/UNI217238/Kokic

Actions required of governments, companies and civil society to implement norms and standards

This Manifesto calls for governments to impose stronger regulations on companies in order to shift the onus for data protection from children to companies and governments. Distributive models of data governance should be promoted in order to provide opportunities for child participation, collaboration, and co-creation. Children should also be afforded meaningful redress mechanisms for violations of data rights. Governments themselves must also put in place rules to restrict the reuse of children's data held by the public sector, and to impose obligations on data intermediary services, drawing on the new European Data Governance Act, which requires publicly available conditions for the re-use of data that are non-discriminatory, proportionate and objectively justified.[182] Governments should ensure data sovereignty of individual children, as required by the EU, and enhanced in the proposed European Data Governance Act.[183]

4. **SHIFT** responsibility for data protection from children to companies and governments.

Enforcement of an international data governance framework for children could be carried out at a number of levels. Whereas consent has become a hallmark of data governance for adults, placing them and their agency at the centre, obtaining meaningful consent from children and sometimes their parents is fraught with difficulties. Key to a truly rights-based approach to accountability would be a reversal of the current burden on children and their advocates to bring challenges against companies, organizations, and governments for breaches of children's data rights, where the onus is on children to prove rights violations. Instead it would require governments to mandate companies to:

- **Produce accessible reports,** audited by an independent third party, on how they are using children's data, putting the onus on them to prove that they are not violating children's rights.

- **Be open and transparent about what measures they have put in place** to monitor and track children's behaviour, how they respond to children's requests to delete their data, how they use and share data collected from children online, and the nature and extent of any filtering mechanisms to protect children from accessing harmful content. It is very difficult to hold companies accountable for their practices related to children's data without much more transparency than is currently provided.[184]

- Require companies and organizations operating across multiple jurisdictions to **apply the highest data protection and child rights protection standards** to their services everywhere, irrespective of children's or their guardians' consent to data processes. Companies need to publicly commit to the highest standards of data protection for children, beyond mere compliance with the law. Given the rapid pace of development of technology and associated data collection, processing and storage practices, companies must proactively ensure that they are acting responsibly and according to child rights principles, even when this is not strictly required by law.

- **Senior company officers need to be held personally liable** for protecting children's data and privacy rights. Making senior company officers personally accountable for breaches of data rights by imposing personal civil penalties could introduce greater incentives to comply with data protection laws. We believe that liability should be commensurate to the level of the decision-making power in the organization or company, and multinational companies based in the West must not be able to appoint national representatives in other countries to take on exclusive liability in this regard. This liability for breaches through gross negligence or disregard for the law, would be a question of fact for DPAs and national courts to determine. This would not be a remedy that exists in isolation from addressing the systems of data protection and privacy that must also be put in place for children, which are necessary to avoid ever reaching a data rights violation that constitutes gross negligence.

- **Consider the development of a fair-trade label as a means of standard setting for companies who respect, protect and promote children's rights in their data processing practices.** In order to achieve the fair-trade label, companies would need to open themselves to audit by an independent body tasked with assessing their adherence to specified child rights-based standards as well as data protection compliance.

- **Businesses should also be proactive in maximising the use of data for children's benefit** by, for example, sharing anonymized data for research purposes where appropriate, and contributing to open data sets for social good, whilst scrupulously applying the Responsible Data for Children principles.

5. **COLLABORATE** with children and their communities in policy building and management of their data.

Evolving internet governance frameworks offer different insights that can inform the development of global data governance, allowing for child and youth participation and empowerment, both in policy development, and in management and control of their data. The Global Commission on Internet Governance, for example, advocates a multi-stakeholder and devolved national model of internet governance, rather than a top-down government-led model.[185] Devolved governance means that different stakeholders across the public and private sectors and civil society should all have power and influence over regulation of children's data, and national governments can make subnational authorities responsible for aspects of data governance in their locality. Distributed governance can be said to mediate between multilateral and multi-stakeholder forms of governance, by adding a way to operationalize notions of collaborative, transparent and bottom-up responses to pressing and complex issues.[186] This idea of distributed governance is thought to allow for freedom for innovation and interoperability, and greater participation and control by data subjects. This model would foresee increased participation of children, their parents and communities in the monitoring of data collection and use by different parties, and greater say in how the data are processed and for which purposes. It would also require increased transparency by those collecting, using and sharing children's data.

Child participation and empowerment should become a permanent feature of all data governance frameworks, not a one-off event. This means that children should be involved in the co-creation of data governance protocols and should be active leaders in the stewardship of, and access to, that data. Lessons could be drawn from data governance models built with indigenous communities. In New Zealand, Maori models of data governance are being incorporated into government data governance systems, allowing space for collective rights and not just individual privacy and ownership rights. This concept demands clear lines of accountability for the collection of data, and calls for both benefit- and power-sharing.[187] Similarly, children are collectively impacted by data gathered on them at scale. They should therefore be accorded accountability mechanisms, benefit- and power-sharing.

Distributed governance could also be achieved at local as well as national levels, for example by building on initiatives such as the ones launched in Amsterdam and Helsinki to produce public AI registers which detail how each city government uses algorithms to deliver services.[188] Data registers could be produced at a local level to detail how educational institutions, hospitals and social welfare services are collecting and processing children's data, including through the use of AI.

Distributed governance models also help to provide greater agency to children in countries with more authoritarian national governments, allowing them to challenge data surveillance practices at a local government level, even where national laws are difficult to challenge for political reasons.

Underpinning the empowerment and participation of children in data governance is the provision of comprehensive digital and data literacy programmes for children, their parents, educators, and the public. Children must be equipped to make informed decisions about the use of their own data, and the implications of giving their consent to data collection by different actors. Done in an age-appropriate way, children (as well as their guardians and educators) can learn and stand to significantly benefit from responsibly used childhood data. Digital literacy programmes should also be inclusive and tailored to meet the needs of children with disabilities, children living in institutions, children on the move, and children from minority ethnic language groups. The draft OECD Recommendation on Children in the Digital Environment recognizes the essential role of digital literacy

Comprehensive overviews of digital literacy frameworks and approaches that include data literacy can be found in Berkman Klein Center report on **Youth and Digital Citizenship+ (Plus)** and UNICEF's **Digital Literacy Scoping Paper**

in supporting children in "understanding how their personal data is collected, disclosed, made available or otherwise used."[189] The need for awareness-raising campaigns on the rights of the child in the digital environment is also echoed by the CRC General Comment No.25.

6. **REPRESENT** children's interests within administrative and judicial processes, as well as redress mechanisms.

Children or their representatives should be able to invoke internationally agreed norms and standards whenever violations of data rights occur. This could be done by ensuring such norms and standards are reflected in national laws, and by creating mechanisms that allow children to seek redress for data rights' violations through their local and national courts, via their ombudsperson for children, or through their local data protection authority (DPA).

There is currently a gap in expertise between the international child rights sector and the international data governance sector which goes in both directions. It is vital that people who work on data governance are trained in children's rights so that they can apply data protection regulations appropriately to child subjects. It is equally crucial that people who work on child rights are trained in data governance, in order to understand the impact of data processing on children's rights, and to hold data controllers and processors accountable, where necessary, to implement the rights of the child.

DPAs at both subnational and national levels should employ staff specialized in children's rights and should all be able to liaise with regional associations of DPAs. Currently the UK Information Commissioner's Office employs staff specialized in children's rights, and has produced the Age Appropriate Design Code (AADC) which guides information society services on how to implement the GDPR in accordance with children's rights. The Dutch Government also released a Code for Children's Rights in 2021, which aims to guide designers and developers of digital products on ensuring their products are rights-based, and is reportedly inspired by the AADC.[190] As noted earlier, where countries do not currently have a DPA, they should be established.

Regional associations of DPAs can also work towards model national laws that are inclusive of children's rights and that work in the context of cultural norms and plural legal traditions. The Global Privacy Assembly should endorse the integration of children's rights into

any new international data governance framework or institution and ensure that children's rights are implemented through its international network of DPAs, with the involvement of children.

Regional bodies such as the European Union should make compliance with specified internationally agreed norms and standards related to children's data rights a prerequisite for any adequacy assessment under laws such as the GDPR, prior to allowing trade of children's data with States outside the EU. States must currently satisfy general data protection requirements and evidence limitations on surveillance of their populations before their data governance is deemed 'adequate' by the EU, and these requirements should be expanded to include special provisions related to children's data rights.

Governments that are signatories to the CRC have a duty to report periodically to the Committee on the Rights of the Child regarding their fulfilment of children's rights within their national legal, regulatory, and policy frameworks. **Governments should include an analysis of their implementation of internationally agreed norms and standards related to children's data rights** in these reports as they relate directly to each of the articles of the CRC, giving due regard to the CRC General Comment 25. Non-profit and multilateral organizations should provide the same information in their alternative reports to the Committee on the Rights of the Child.[191]

Internationally agreed norms and standards related to children's data rights should be embedded within existing human rights impact assessments, such as those carried out by Ranking Digital Rights, in recognition of the fact that one third of users of the internet are children; most technology companies will therefore have a sizeable user base under the age of 18 whose rights they have a legal duty to protect, promote and respect. Technology companies should integrate data management in their corporate social responsibility reporting, and should publish a data strategy that outlines children's rights to privacy, data protection, and the principles for management of children's data throughout the life cycle.

7. **PROVIDE** adequate resources to implement child-inclusive data governance frameworks.

Allocation of sufficient financial and human resources by governments, the private sector, and the development sector is fundamental to the incorporation of children's rights into any current or future global data governance regime. As we mentioned above, it is essential that Data Protection Authorities (DPAs) employ staff with expertise in child rights, and that they visibly and distinctly address children's data, and actively enforce regulatory laws to protect children. This means that governments must ensure funding is available to train DPA staff in child rights, as well as for dedicated child rights specialist positions within each DPA.

Technology companies providing services that may be accessed by children should also ensure they have staff trained on child rights as well as a focal point for children's data governance. This focal point must be accessible by children and their representatives who wish to make subject access requests, or to seek clarification about other aspects of the use and management of their data by the company. Large teams of staff trained in children's data rights may be required where companies have extensive regional or global reach.

Donors funding humanitarian or development projects that involve data collection from children should require both a data protection impact assessment and a child rights impact assessment from their applicants as a prerequisite for funding. These impact assessments should draw on the RD4C Principles, and the CRIA framework which is a tool for translating the CRC and the best interests of the child principle into practice.[192]

Enablers of good governance of children's data

This Manifesto identifies some key enablers of good governance of children's data, which includes the use of policy innovation and facilitation of cross-country learning in implementing children's data rights at national and local levels. There also remain some urgent knowledge gaps that need to be filled through further research to ensure that data governance regulations are evidence-based. Finally, we call for international collaboration for children's data governance, that is inclusive of all regions and allows for knowledge-sharing between the Global North and the Global South in both directions.


© UNICEF/UNI344477/

8. **USE** policy innovation in data governance to solve complex problems and accelerate results for children.

Policy innovation can help public authorities to make the most of data, while at the same time safeguarding children's rights and data protection principles and standards. The need for governments to innovate is becoming a central tenet of public policymaking, including in policies related to data. Changes in how policies are conceptualised, developed and tested have the potential to improve policy efficiency and outcomes, solve complex problems, and accelerate results for children. Current examples that can be built upon include:

Regulatory sandboxes

Regulatory sandboxes allow regulators to engage with innovators working on products and services that are likely to be used by children and vice versa. The UK Information Commissioner's Office (ICO) is engaging with innovators intending to implement the Age Appropriate Design Code.[193] Current initiatives accepted by the ICO sandbox include a trial of technology that combines age estimation tools with content-moderated e-sport membership platforms for under-18s with parental consent options, including the use of age estimation for parental consent. Another trial involves an initiative from a privacy and consent management platform that aims to help companies become compliant with data privacy regulations worldwide, which is seeking to enhance its consent management platform by providing child privacy consent management.[194]

The success of the UK Financial Conduct Authority's regulatory sandbox has led towards efforts to create a global regulatory sandbox which would facilitate cross-jurisdictional referral systems, promote regulatory convergence, and help firms understand the regulatory environment in selected key markets.[195] A global regulatory sandbox focused on children's data could be a useful mechanism for ensuring that regulations work across borders and importantly comply with international human rights and children's rights laws and standards.

Data trusts

Data can be protected, managed, and overseen on behalf of children through the use of data trusts which provide independent, fiduciary stewardship of children's data. The Open Data Institute defines stewardship of data as "collecting, maintaining, and sharing it, and in particular deciding who has access to it, under what conditions and to whose benefit."[197] Data trusts have been noted as a personal data intermediary with significant potential by the European Commission in the 2020 European strategy for data. They can be used at a city or local level to allow for community consent to data collection where individual consent may not be feasible, but it is still important for citizens to be involved in decisions on how their community's data is used.[198] In the case of children some thought would need to be given to parental consent in relation to data trusts, and the age at which children should be deemed competent to consent on their own behalf.

What is a data fiduciary?

A data fiduciary relationship is one in which the child is dependent on a 'data steward' to decide when and how their data can be used and by whom, and to manage the child's data on their behalf. The data steward typically has a duty of care, loyalty and sometimes confidentiality, to the child.[196]

Data intermediaries

The EU Data Governance Act[199] highlights the importance of data intermediaries and data altruism organizations as data governance mechanisms. The MyData[200] operator is a human-centric model of data intermediary that provides a reference framework, including functional elements of identity management. The MyData model could be adapted to ensure that it meets the specific needs and abilities of children at different development stages and ages. MyData Global proposes that the use of data intermediaries can help to empower children by improving their right to self-determination regarding their personal data.


© UNICEF/UN0303659/Arcos

9. **BRIDGE** knowledge gaps in the realm of data governance for children. There are some urgent knowledge gaps that need further research to ensure that data governance regulations are evidence-based.

Through the process of the development of this Manifesto, some critical knowledge gaps were identified in relation to children's data governance. Filling these gaps through research, analysis and expert consultations will allow policy makers, data practitioners and child rights' advocates to develop better targeted policies and solutions for children.

- **There is a need for the development of a 'typology of harms'** that can enable research and evidence generation of the types of harms caused by breaches of children's data rights and privacy rights.

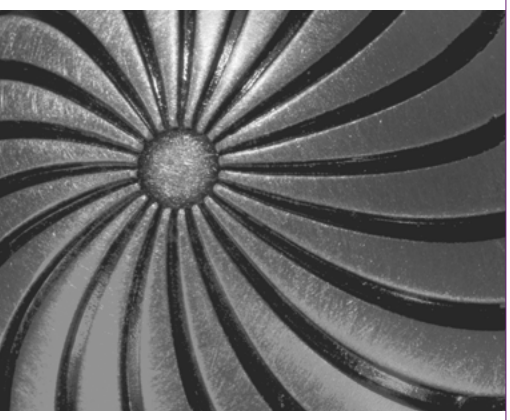
- **The concept of "consent" to data processing needs to be better understood and defined,** including consent from children at different ages and stages of childhood and in different contexts. The concept of informed and meaningful parental consent to data processing also needs to be revisited from a child rights perspective. An assessment should be made of parents' or caregivers' capacity to make a decision in the best interests of the child related to data collection, and whether this is an unreasonable burden to place on them.

- **Further scholarship is needed to address some of the emerging tensions between children's rights to data protection and privacy with their other rights.** In some situations, children's data could be collected and processed excessively while aiming to protect them from serious harms such as sexual exploitation and abuse, or while aiming to promote their rights to access education and health care. There is a need for detailed guidance on how to apply the necessity and proportionality test to children's data rights.

- **There is a need to elaborate on the application of the concept of the "best interests of the child"** and of the child's "well-being", in the context of data processing, profiling, nudging, and the right to self-determination. It would be useful for a set of indicators to be developed in this regard that can be used by policymakers as well as the industry.

- **Monitoring and evaluation of the impact of different approaches to data protection regulation on children should be carried out,** to form a shared evidence base and to improve good practice going forwards.

This research will be essential in ensuring clarity in legal concepts related to children's data governance, and their implementation. This Manifesto calls on the data governance community to work towards as much legal certainty as possible to provide the parameters for good governance of children's data. If legislation on data is not clear, then meaningful governance becomes close to impossible. This issue is especially relevant for childhood data, where potential harms can be significantly more severe than is the case with other personal data.



10. **STRENGTHEN** international collaboration for children's data governance and promote knowledge and policy transfer among countries.

This Manifesto echoes recommendations made to the G20 in 2020 that **governments should aim for multilateral consensus on data governance**, and calls for greater global coordination in terms of law and policy.[201] Uncoordinated national-level data governance laws can lead to competing assertions of jurisdiction and conflict of laws. This prevents actors from properly addressing abuses online and favours the rule of the strongest, further widening the divide between the Global North and the Global South.

This Manifesto calls for increased collaboration between data governance actors internationally, to allow for governments and other leaders to learn from each other regarding innovative policy approaches to incorporating children's rights in data governance frameworks. It is crucial that this knowledge transfer is not just from the Global North to the Global South, but that emerging data governance regimes that can be usefully applied to children are also considered in global governance regimes. For example, Ubuntu philosophy from sub-Saharan Africa (see page 76) can be used to inform policymaking related to automated decision-making[202] and its use on children; or the Non-Aligned Movement – a forum of 120 developing world States[203] – could be harnessed to ensure the interests of children from the Global South are included in global data governance mechanisms. Lessons can also be learned from the Maori approach to collective ownership of data mentioned above.[204]

There should also be space for international collaboration and leadership across civil society organizations in setting standards for children's data governance, challenging the binary choice between government regulation and industry self-regulation. So far, we have seen an emphasis on industry self-regulation, largely due to an assumption that expertise is concentrated in the private sector, and that the public sector is unable to keep up with the pace of innovation. This overlooks the increasingly important role played by civil society organizations which also have considerable expertise, are not constrained by the bureaucracy of the public sector, and have core values that are centred in children's rights. The CRC General Comment 25 states that governments should systematically involve civil society in the development and implementation of laws and policies related to children's rights in the digital environment.


© UNICEF/UNI74752/Pirozzi

Ubuntu as an ethical human rights framework for artificial intelligence governance

Mhlambi[205] argues that "the relational sub-Saharan African philosophy of ubuntu reconciles the ethical limitations of rationality as personhood by linking one's personhood to the personhood of others". Ubuntu can be used to show that the harms caused by artificial intelligence, and automated decision-making systems (ADMS) in particular, are in essence violations of ubuntu's relational personhood and relational model of the universe. Postcolonial African philosophy argues that the economic, political, and social inequalities that dominate the processes that shape the creation of artificial intelligence are neocolonial and are assaults on human dignity. Mhlambi makes technical and policy recommendations for addressing the negative effects of artificial intelligence systems as follows:

- The data collected from users that powers ADMS should be used for public good and made available to the public in ways that protect privacy and promote the well-being of society;
- Communities should be able to treat their data as intellectual property that can be licensed or revoked from online platforms;
- Greater funding and access to technical skill sets must be made available to the most disenfranchised;
- The ways in which algorithms make considerations should allow users to be able to directly shape the recommendations they receive; and
- Technology companies should tailor recommendations with agreed upon social ideals based on human dignity and social cohesion.[206]

Civil society organizations could take an alternative approach by engaging in the development of collaborative standards for children's data in the open. This may prove to be a fruitful mechanism for civil society to put forward detailed standards related to children's data governance, grounded in international human and children's rights. Open source development focuses more on output than process, and would be a fluid way to promote collaboration across jurisdictions to enable the collective writing of international standards related to children's data rights.

This Manifesto is the beginning of a process, and the first step in ensuring that children's rights are given due weight in data governance legal frameworks and processes as they evolve around the world.

The way forward

We hope that this will be a living document that is built upon as the data landscape for children changes in the future. Each of the working group members will take this Manifesto forwards in their own work and in their own regions, and much work remains to be done. We hope that this document encourages those who are concerned about child welfare and their rights to use our findings and recommendations and to develop more concrete action points. Some of these have already been brought to our attention during the process of the development of the Manifesto. They could include:

- Development of concrete guidance on how to work at national and subnational levels to ensure that children's rights are included in data governance regulations and strategies;
- Development of model regulations on data governance that include children's rights and interests;
- Development of guidance for the private sector to ensure they incorporate the highest standards of data governance for children into their policies and practices; and
- Development of impact assessment tools to measure the level of compliance and impact of data collection and processing on children.

Now that global attention is starting to turn to the need to improve governance of data and of the technology sector in general for everyone, it is critical that children's rights are given due consideration and a central role in new envisaged legal and regulatory landscapes.

Endnotes

1. United Nations Convention on the Rights of the Child. https://www.ohchr.org/en/professionalinterest/pages/crc.aspx

2. UK Children's Commissioner, "Who knows what about me? A Children's Commissioner report into the collection and sharing of children's data," November 2018. https://www.childrenscommissioner.gov.uk/wp-content/uploads/2018/11/cco-who-knows-what-about-me.pdf

3. European Commission, What is personal data?: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

4. Thuret-Benoist, M. (2019). What is the difference between personally identifiable information (PII) and personal data? TechGDPR. https://techgdpr.com/blog/difference-between-pii-and-personal-data/#:~:text=In%20a%20nutshell%2C%20PII%20refers,to%20an%20identifiable%2C%20living%20individual.

5. Federal Trade Commission (2013). "Revised Children's Online Privacy Protection Rule Goes Into Effect Today." https://www.ftc.gov/news-events/press-releases/2013/07/revised-childrens-online-privacy-protection-rule-goes-effect

6. Committee on the Rights of the Child, General comment No. 25 (2021) on children's rights in relation to the digital environment. CRC/C/GC/25 https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx

7. McDonald, S. (2020). "Data Fiduciaries for Protecting Children's Data." https://www.unicef.org/globalinsight/reports/fiduciary-approach-child-data-governance

8. Livingstone, S. Stoilova, M. and Nandagiri, R. (2019). Children's data and privacy online: Growing up in a digital age. An evidence review. London: London School of Economics and Political Science. https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review.pdf; UNICEF East Asia and Pacific (2020). Our Lives Online: Use of social media by children and adolescents in East Asia - opportunities, risks and harms https://www.unicef.org/eap/reports/our-lives-online

9. Livingstone et al. (2019). https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review.pdf

10. Livingstone, S. (2019) Social Media Data: tracing family and children's data flows. https://blogs.lse.ac.uk/parenting4digitalfuture/2019/07/17/social-media-data/

11. Wlosik, M. (2020). What is a data broker and how does it work? https://clearcode.cc/blog/what-is-data-broker/

12. Person, J. (2020). "Safeguarding-in-schools data sharing and web monitoring in the Prevent programme." Defend Digital Me. (Unpublished and confidential report)

13. Lomas, N. (2019). "Google completes controversial takeover of DeepMind Health", TechCrunch. https://techcrunch.com/2019/09/19/google-completes-controversial-takeover-of-deepmind-health/.

14. Cox, K. (2019). "It's the user's fault if a Ring camera violates your privacy, Amazon says." ArsTechnica. https://arstechnica.com/tech-policy/2019/11/cops-can-keep-ring-footage-forever-share-it-with-anyone-amazon-confirms/

15. Day, E. (2020). Working Paper on Children's Health Data. (Forthcoming). Citing Kristin Bergtora Sandvik (2020) Wearables for something good: Aid, dataveillance and the production of children's digital bodies, *Information, Communication & Society*, DOI: 10.1080/1369118X.2020.1753797

16. The case study was replicated in this format with the permission of Sitra. For more information see: https://www.sitra.fi/en/topics/fair-data-economy/

17. Sitra (2020). Discover your digital profile. https://digiprofiilitesti.sitra.fi/

18. UN/CRC/C/GC/16. General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights, item 16, p. 6. https://www2.ohchr.org/english/bodies/crc/docs/CRC.C.GC.16.pdf

19. Hartung, P. (2020). "The Children's rights-by-design (CRbD) standard for data use by tech companies." https://www.unicef.org/globalinsight/reports/childrens-rights-design-new-standard-data-use-tech-companies. Note: this section draws heavily from Hartung's work.

20. Berman, G. and Albright, K. (2017). "Children and the Data Cycle: Rights and Ethics in a Big Data World" *Innocenti Working Paper* No. 2017-05, UNICEF Office of Research - Innocenti. https://www.unicef-irc.org/publications/907/

21. Lansdown, G. (2005). "The Evolving Capacities of the Child." Save the Children and UNICEF Innocenti Research Centre. https://www.unicef-irc.org/publications/pdf/evolving-eng.pdf

22. Richards, N. (2008). Intellectual Privacy, 87 *Texas Law Review*, 387, 388–391.

23. Richards, N. (2008). The Dangers of Surveillance, 126 Harvard Law Review 1934, 1935.

24. ILO Minimum Age Convention, 1973 (No. 138).

25. Richards, N. (2008). Intellectual Privacy, 87 Texas Law Review, 387, 388–391.

26. Richards, N. (2008). The Dangers of Surveillance, 126 *Harvard Law Review* 1934, 1935)

27. United Nations (1989) Convention on the Rights of the Child General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1). https://www2.ohchr.org/English/bodies/crc/docs/GC/CRC_C_GC_14_ENG.pdf; Guidelines on Determining the Best Interests of the Child. https://www.unhcr.org/4566b16b2.pdf

28. United Nations (1989) Convention on the Rights of the Child. https://www.ohchr.org/en/professionalinterest/pages/crc.aspx

29. United Nations Children's Fund and International Telecommunication Union (2020). "How many children and young people have internet access at home? Estimating digital connectivity during the COVID-19 pandemic." UNICEF, New York. https://data.unicef.org/resources/children-and-young-people-internet-access-at-home-during-covid19/

30. Radesky, Jenny et al. (2020). "Digital Advertising to Children", Pediatrics 146, n. 1, July 2020; WHO (2016). "Tackling Food Marketing to Children in a Digital World: Trans-Disciplinary Perspectives. Children's Rights, Evidence of Impact, Methodological Challenges, Regulatory Options and Policy Implications for the WHO European Region"; Social Issues Research Centre (2009). "The Impact of the Commercial World on Children's Wellbeing: Report of an Independent Assessment".

31. Montgomery, K.C., Chester, J., and Kopp, K. (2020). "Data Governance for Young People in the Commercialized Digital Environment", UNICEF Office of Global Insight and Policy. https://www.unicef.org/globalinsight/reports/data-governance-young-people-commercialized-digital-environment

32. Montgomery, Chester, and Kopp (2020); Nyst, C. (2018). "Children and digital marketing: Rights, risks and responsibilities", UNICEF.

33. Montgomery, Chester, and Kopp (2020).

34. Montgomery, Chester, and Kopp (2020).

35. Bankston, K., and Soltani, A. (2014). "Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones" January 9, 2014, Yale Law Journal. https://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones

36. UN Office of the High Commissioner for Human Rights, press release (2019). UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736

37. Ennis, H., Esetevez, A., and Mariani, J. (2019). "National security and technology regulation: Government regulations for emerging technology", *Deloitte Insights.*

38. Raftree, L.(2019). "A discussion on WFP-Palantir and the Ethics of Humanitarian Data Sharing", Digital Impact. https://digitalimpact.io/a-discussion-on-wfp-palantir-and-the-ethics-of-humanitarian-data-sharing/

39. Raftree, L., Day, E., and Byrne, J. (2020). "COVID-19: A spotlight on chidren's data governance gaps". UNICEF Office of Global Policy and Insight. https://www.unicef.org/globalinsight/media/1111/file/UNICEF-Global-Insight-data-governance-covid-issue-brief-2020.pdf

40. Vosloo, S., Penegos, M., and Raftree, L. (2020). "COVID-19 and children's digital privacy". UNICEF Office of Global Insight and Policy. https://www.unicef.org/globalinsight/stories/covid-19-and-childrens-digital-privacy

41. Day, E. (2020). "Children's Health Data Governance," October 2020. (Forthcoming99999999999)

42. Moore, S., Tassé, A. M., Thorogood, A., Winship, I., Zawati, M., & Doerr, M. (2017). "Consent Processes for Mobile App Mediated Research: Systematic Review". *JMIR mHealth and uHealth*, 5(8), e126. https://doi.org/10.2196/mhealth.7014

43. Day, E. (2020).

44. UNICEF (2021). COVID-19 and School Closures: One year of education disruption. https://data.unicef.org/resources/one-year-of-covid-19-and-school-closures/

45. Barrett, L. (2020). "Issue Brief on Student Data Governance", UNICEF Office of Global Insight and Policy. https://www.unicef.org/globalinsight/reports/governance-student-data

46. Google. (2020) Google Workspace for Education Privacy Notice https://workspace.google.com/intl/pt-BR/terms/education_privacy.html

47. Google (2020) Privacy and Security Center. https://edu.google.com/intl/pt-BR/why-google/privacy-security/?modal_active=none

48. Hartung, P. (2020). "The Children's rights-by-design (CRbD) standard for data use by tech companies". UNICEF Office of Global Insight and Policy. https://www.unicef.org/globalinsight/reports/childrens-rights-design-new-standard-data-use-tech-companies

49. Bulger, M. (2016). "Personalized Learning: The Conversations We're Not Having", *Data & Society, Working Paper*. https://datasociety.net/pubs/ecl/PersonalizedLearning_primer_2016.pdf

50. Persson, J. (2020). Key Informant Interview

51. Schneier, B. (2018). Schneier on Security, How Surveillance Inhibits Freedom of Expression, Schneier.com, November 26, 2018.

52. Kingaby, H. and Kaltheuner, F. (2020). "Policy Brief: Ad Break for Europe. The Race to Deregulate Advertising and Online Space". https://assets.mofoprod.net/network/documents/Ad_Break_for_Europe_FINAL_online.pdf

53. Sandik, K. (2020). Humanitarian Wearables: Digital Bodies, Experimentation and Ethics. https://link.springer.com/chapter/10.1007/978-3-030-36319-2_6 Springer

54. UNICEF (2019). Faces, Fingerprints and Feet. https://data.unicef.org/resources/biometrics/

55. Raftree, L. (2020). "Digital Safeguarding for Migrating and Displaced Children". Save the Children, Migration and Displacement Initiative. https://resourcecentre.savethechildren.net/node/18477/pdf/mdi_digital_final_rgb_rev_051120.pdf

56. UNHCR (2020). "Figures at a Glance". https://www.unhcr.org/figures-at-a-glance.html.

57. European Union Agency for Fundamental Rights (2018). "Age assessment and fingerprinting of children in asylum procedures. Minimum age requirements concerning children's rights in the EU". https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-minimum-age-asylum-procedures_en.pdf.

58. European Commission (2020). COM(2020) 614 final, Amended proposal for a Regulation of the European Parliament and of the Council of the establishment of 'Eurodac' for the comparison of biometric data for the effective application of Regulation (EU) XXX/XXX [Regulation on Asylum and Migration Management] and of Regulation (EU) XXX/XXX [Resettlement Regulation], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulations (EU) 2018/1240 and (EU) 2019/818. https://ec.europa.eu/info/sites/info/files/proposal-regulation-biometric-data_en.pdf.

59. Raftree, L. (2020).

60. Bughin, J., et al. (2018). 'Notes from the AI Frontier: Modeling the Impact of AI on the World Economy', https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Notes%20from%20the%20frontier%20Modeling%20the%20impact%20of%20AI%20on%20the%20world%20economy/MGI-Notes-from-the-AI-frontier-Modeling-the-impact-of-AI-on-the-world-economy-September-2018.ashx

61. Noble, Safiya Umoja (2018). Algorithms of oppression: How search engines reinforce racism. New York: New York University Press.

62. UNICEF (2020). Policy Guidance on AI for Children. https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf

63. De La Garza, A. (2020). "Coronavirus Researchers Are Using High-Tech Methods to Predict Where the Virus Might Go Next" February 11, 2020. *TIME*. https://time.com/5780683/coronavirus-ai/

64. Lee, K.F. (2020). "COVID-19 will Accelerate the AI Health Revolution" May 5, 2020, WIRED. https://www.wired.com/story/covid-19-will-accelerate-ai-health-care-revolution/

65. Save the Children and Boston Consulting Group (2019). Predicting Displacement. https://resourcecentre.savethechildren.net/node/14290/pdf/predicting_displacement_report_-_save_the_children_mdi.pdf

66. Berman and Albright (2017). https://www.unicef-irc.org/publications/pdf/IWP_2017_05.pdf

67. Barrett, L. (2020). https://www.unicef.org/globalinsight/reports/governance-student-data

68. Angwin, J. et al. (2016). "Machine Bias" *ProPublica*: May 23, 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

69. Data Science and Ethics Group (2020). "A Framework for the Ethical Use of Advanced Science Methods in the Humanitarian Sector". https://www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/dseg_ethical_framework_april_2020.pdf

70. Berkman Klein Center for Internet & Society, (2020). 'Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI', https://cyber.harvard.edu/publication/2020/principled-ai

71. Dignum, V., Penagos, M., Pigmans, K., and Vosloo, S. (2020). Policy Guidance on AI for Children, UNICEF, New York.

72. UNICEF (2020). Policy Guidance on AI for Children. https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf

73. Berman and Albright (2017) https://www.unicef-irc.org/publications/pdf/IWP_2017_05.pdf

74. Wang, T. (2020). "You are not your data but your data is still you". Deep Dives. https://deepdives.in/you-are-not-your-data-but-your-data-is-still-you-b41d2478ece2

75. Ghosh, D. (2018). "What is Microtargeting and what is it doing in our politics?", *Internet Citizen*, Mozilla Foundation. https://blog.mozilla.org/internetcitizen/2018/10/04/microtargeting-dipayan-ghosh/

76. Kidron, B. Evans, A., Afia, J. (2018). "Disrupted Childhood: The Cost of Persuasive Design", 5Rights Foundation. https://5rightsfoundation.com/static/5Rights-Disrupted-Childhood.pdf

77. Ghosh, D. (2018). https://blog.mozilla.org/internetcitizen/2018/10/04/microtargeting-dipayan-ghosh/

78. Raftree, L. (2019). "Digital and Social Media for Social and Behaviour Change Communication" iMedia Associates. https://imediaassociates.org/app/uploads/2019/07/Digital-and-Social-Media-for-SBCC-March-2019.pdf

79. See The Communications Initiative for a wide variety of social and behaviour communication strategies and techniques, including some that use digital marketing approaches.

80. See Data & Society on media manipulation and disinformation. https://datasociety.net/research/media-manipulation/

81. Guay, J., Gray, S., Rhynard-Geil, M., Inks, L. (2019). "The Weaponization of Social Media: How social media can spark violence and what can be done about it", Mercy Corps.

82. UNICEF (2020). "Policy Guidance on AI for Children". https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf

83. Hartung, P. (2020). "The children's rights-by-design (CRbD) standard for data use by tech companies", UNICEF Office of Global Insight and Policy. https://www.unicef.org/globalinsight/reports/childrens-rights-design-new-standard-data-use-tech-companies

84. Government of India (2020). Report by the Committee of Experts on Non-Personal Data Governance Framework. https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/08/mygov_159453381955063671.pdf

85. Young, A. (2020). "Children's Group Data Governance". https://www.unicef.org/globalinsight/reports/responsible-group-data-children; Taylor, L, Floridi, L and van der Sloot, B. (2017) "Introduction: A New Perspective on Privacy", in L. Taylor, L. Floridi and B. van der Sloot (eds.), Group Privacy: New Challenges of Data Technologies. Dordrecht: Springer.

86. Young, A. (2020). https://www.unicef.org/globalinsight/reports/responsible-group-data-children

87. Halliman, D. and de Hert, P. (2017). "Genetic Classes and Genetic Categories: Protecting Genetic Groups through Data Protection Law," in L. Taylor, L. Floridi and B. van der Sloot (eds.), Group Privacy: new challenges of data technologies. Dordrecht: Springer 2017.

88. Taylor, Floridi and van der Sloot (2017).

89. Bode, K. (2020). "Researchers Find 'Anonymized' Data Is Even Less Anonymous Than We Thought." *Motherboard*. February 3, 2020. https://www.vice.com/en/article/dygy8k/researchers-find-anonymized-data-is-even-less-anonymous-than-we-thought

90. Livingstone, S. and Stoilova, M. (2021). Content, contact, conduct and contract – updating the 4Cs of online risk, *Children Online Research and Evidence*, 8 March 2021.

91. Kardefelt-Winther, D., Day, E., Berman, G., Witting, S. and Bose, A. (2020). Encryption, Privacy and Children's Right to Protection from Harm, UNICEF Office of Research – *Innocenti Working Paper* WP-2020-14.

92. Kardefelt-Winther, Day, Berman, Witting, and Bose, (2020). 0

93. European Commission (2010). Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive). Available at https://ec.europa.eu/digital-single-market/en/protection-minors-avmsd

94. Reward Foundation (2020). Age Verification Conference Report.

95. Nash, V. (2013). Effective age verification techniques: Lessons to be learnt from the online gambling industry, Oxford Internet Institute.

96. Day, E., and Galea Baron, J., Digital Age Verification Tools and Children's Rights Online: A Discussion Paper. (forthcoming 2021)

97. Internet Matters (ND). Set Up Kids' Tech Devices: E-safety Checklist.

98. Chandler S., and Jansen, M. (2020). The bets parental control apps for Android and iOS Digital Trends. August 27, 2020.

99. Feal, A. et al. (2020). Angel or Devil? A Privacy Study of Mobile Parental Control Apps. *Proceedings on Privacy Enhancing Technologies*, Sciendo, 2020(2) 314-335.

100. Kardefelt-Winther, Day,, Berman, Witting, and Bose, (2020).

101. Lansdown (2005). https://www.unicef-irc.org/publications/pdf/evolving-eng.pdf

102. Livingstone, Stoilova, and Nandagiri (2019). https://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf

103. Livingstone, Stoilova, and Nandagiri (2019). https://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf

104. Stoilova, M., Livingstone, S. Nandagiri, R. (2020). "Children 's expectations regarding fair treatment of their personal data: what policy makers should know", P*arenting for a Digital Future,* September 19, 2020.

105. UNICEF (2017). Implementation Handbook for the Convention on the Rights of the Child: Third Edition.

106. Harman, J. (2020). "Note on Children, Age and Data Protection" (unpublished)

107. Young (2020). https://www.unicef.org/globalinsight/reports/responsible-group-data-children.

108. UNICEF East Asia and Pacific (2020). https://www.unicef.org/eap/reports/our-lives-online

109. Harman (2020).

110. Information Commissioner's Office (2020). Age-Appropriate Design Code, UK ICO. https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/

111. See the UN Convention on the Rights of the Child and the UN Declaration on Human Rights.

112. McDonald, S.M. (2021). "A Fiduciary Approach to Child Data Governance", UNICEF Office of Global Insight and Policy. https://www.unicef.org/globalinsight/reports/fiduciary-approach-child-data-governance;National Forum on Education Statistics (2020). "Forum Guide to Data Governance", US Department of Education. Washington, DC: National Center for Education Statistics. https://nces.ed.gov/pubs2020/NFES2020083.pdf

113. The political economy of children's data offers a wide set of considerations. Data cannot be de-linked from power and institutions, and data governance mechanisms should be careful to avoid digital data being used to cement power and profits for the privileged. , A key reason why an international data governance regime for children is needed, is to ensure that one nation or region's governance framework does not dominate the globe due to disproportionate economic and political power. Rather, children's data should be subject to an international legal and policy regime applying international human rights and child rights laws and norms that have already been widely negotiated and adopted around the world.

114. Tisne, M. and Schaake, M. (2020). The Data Delusion: Protecting Individual Data Isn't Enough When The Harm is Collective. https://medium.com/@marietje.schaake/the-data-delusion-protecting-individual-data-isnt-enough-when-the-harm-is-collective-13343b33f81f

115. Council of Europe (2020). Guidelines on Children's Data Protection in an Education Setting. https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b

116. See UNICEF and The Danish Institute for Human Rights (2013). Children's Rights in Impact Assessments: A guide for integrating children's rights into impact assessments and taking action for children, UNICEF Geneva and DIHR, Copenhagen.

117. European Union (2016). EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

118. Deloitte LLP (2018). A new era for privacy: GDPR six months on; Renieris, E., (2020). The GDPR at Two – Global Floor or Global Ceiling?. Berkman Klein Center for Internet & Society on Medium.

119. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (TFEU) [2016] OJ C202/1.

120. Charter of Fundamental Rights of the European Union, 2012/C 326/02.

121. The examples below are paraphrased from: Taylor, L. (2020). Public actors without public values: legitimacy, domination and the regulation of the technology sector, SocArXiv papers. https://doi.org/10.31235/osf.io/gtw2x

122. Schwartz, P. and Peifer, K-N., "Transatlantic Data Privacy Law", *Georgetown Law Journa*l, Vol 106:1, 2017.

123. Since the 2014 AU Convention was drafted the global child rights community has agreed to replace the term 'child pornography' with 'child sex abuse materials' to reflect the criminal nature of these materials and to distinguish them from legal forms of pornography depicting adults.

124. List of countries which have signed/ratified/acceded to the African Union Convention on Cybr Security and Personal Data Protection (updated June 2020). Available at: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

125. Prateek, S., and Bhanu, N. (2021). Artifical intelligence needs assessment survey in Africa. UNESCO 2021.

126. Greenleaf, G. (2014). "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories", *Journal of Law*, Information and Science 4. https://www.researchgate.net/publication/272236641_Sheherezade_and_the_101_Data_Privacy_Laws_Origins_Significance_and_Global_Trajectories

127. APEC Privacy Framework 2015. Section V. 26.

128. Brzytwa, E. (2015). Addressing the Costs of Data Localization Requirements – Can APEC Lead the Way?

129. APEC Privacy Framework 2015. Section V. 26

130. UNCTAD (2020). *Data Protection and Privacy Legislation Worldwide*. United Nations Conference on Trade and Development. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

131. Buttarelli, G. (2019). Privacy 2030: A Vision for Europe. (2019) Institute of Advanced Privacy Professionals (IAPP). https://iapp.org/resources/article/privacy-2030/

132. Buttarelli (2019). https://iapp.org/resources/article/privacy-2030/

133. Federal Trade Commission (ND). Complying with COPPA: Frequently asked questions. https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0

134. Nguyen, T. (2017). GDPR Matchup: The Children's Online Privacy Protection Act, Institute of Advanced Privacy Professionals (IAPP). A proposal to update COPPA was tabled by the FTC in 2020 and this may result in raising the age from 13 to 16.

135. Greenleaf (2019). https://it.scribd.com/document/411861387/Global-data-privacy-laws-2019

136. Information Commissioner's Office (2020). https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/executive-summary/

137. Information Commissioner's Office (2020). https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/executive-summary/

138. People's Republic of China (2018). E-Commerce Law of the People's Republic of China. https://ipkey.eu/sites/default/files/documents/resources/PRC_E-Commerce_Law.pdf

139. TransAsia Lawyers (2019). China's First Regulation on the Protection of Children's Personal Information. https://www.lexology.com/library/detail.aspx?g=8a1da201-15a8-4e15-8c33-64fda8fbf621

140. Gladicheva, V. et al. (2019). Around the globe, children's privacy, security emerges as key area of focus for regulators. https://mlexmarketinsight.com/insights-center/editors-picks/area-of-expertise/data-privacy-and-security/around-the-globe,-childrens-privacy,-security-emerges-as-key-area-of-focus-for-regulators

141. Justice K. S. Puttsawamy and Anr. v. Union of India and Ors. (Writ Petition (Civil) No. 494 of 2012), cited in Potter, A. (2019). Privacy rights for children in APAC, One Trust Data Guidance. https://www.dataguidance.com/opinion/international-privacy-rights-children-apac

142. Burman, A. (2020). What Is in India's Sweeping Personal Data Protection Bill?, Carnegie India.

143. Gladicheva, et al (2019). https://mlexmarketinsight.com/insights-center/editors-picks/area-of-expertise/data-privacy-and-security/around-the-globe,-childrens-privacy,-security-emerges-as-key-area-of-focus-for-regulators

144. The Protection of Personal Information Act, 2013 (the "POPIA") was paused in 2013 due to the enactment of the GDPR and revised to accord many of the GDPR provisions. The Act came into force following this revision in July 2020.

145. World Wide Web Foundation (2017). Personal Data: An overview of low and middle income countries. http://webfoundation.org/docs/2017/07/PersonalData_Report_WF.pdf

146. Haataja et al. (2020). Public AI Registers, Realising AI transparency and civic participation in government use of AI. https://uploads-sslwebflowcom/5c8abedb10ed656ecfb65fd9/5f6f334b49d5444079726a79_AI%20Registers%20-%20White%20paper%201.0.pdf

147. Buttarelli (2019). https://iapp.org/resources/article/privacy-2030/

148. Ranking Digital Rights (2019). Corporate Accountability Index. https://rankingdigitalrights.org/index2019/

149. Hern, A. (2020). 'Antiquated process': data regulator onobtaining Cambridge Analytica warrant, The Guardian. 24 Nov 2020.

150. Templafy (2018). GDPR Compliance: US Companies Following EU Standards, Enterprise IT. https://info.templafy.com/blog/gdpr-compliance-us-companies-following-eu-standards

151. Zimmeck, S. et al. (2019). "MAPS: Scaling Privacy Compliance Analysis to a Million Apps", *Proceedings on Privacy Enhancing Technologies*: 2019 (3):66-86

152. Schaake, M. (2020). "The Lawless Realm: Countering the Real Cyberthreat", *Foreign Affairs*, November/December 2020.

153. Information Commissioner's Office (ND). Guide to Data Protection: How should we draft our privacy information? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/how-should-we-draft-our-privacy-information/

154. Council of Europe (2020). https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b

155. Ahmed, U. and A. Chander (2015). "Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-Border Data Flows". E15 Initiative. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum. GSMA (2019) Smart Data Privacy Laws: Achieving the Right Outcomes for the Digital Age, GMSA June 2019.

156. GSMA (2019). Smart Data Privacy Laws: Achieving the Right Outcomes for the Digital Age. https://www.gsma.com/publicpolicy/wp-content/uploads/2019/06/GSMA_Smart-Data-Privacy-Laws_Report_June-2019.pdf

157. GSMA (2019). https://www.gsma.com/publicpolicy/wp-content/uploads/2019/06/GSMA_Smart-Data-Privacy-Laws_Report_June-2019.pdf

158. Congressional Research Service (2019). Data Flows, Online Privacy, and Trade Policy. https://fas.org/sgp/crs/row/R45584.pdf

159. Chakravorti, B., Bhalla, A., and Chaturvedi, R.S. (2019). "Which Countries are Leading the Data Economy?", *Harvard Business Review*. https://hbr.org/2019/01/which-countries-are-leading-the-data-economy?utm_medium=social&utm_source=twitter&utm_campaign=hbr

160. Fay, R. (2019). Digital Platforms Require a Global Governance Framework, Centre for International Governance Innovation.

161. The Economist briefing (2020). A Grand Bargain: Democracies must team up to take on China in the technosphere. https://www.economist.com/briefing/2020/11/19/democracies-must-team-up-to-take-on-china-in-the-technosphere

162. The Economist briefing (2020).https://www.economist.com/briefing/2020/11/19/democracies-must-team-up-to-take-on-china-in-the-technosphere

163. Greenleaf (2014). https://www.researchgate.net/publication/272236641_Sheherezade_and_the_101_Data_Privacy_Laws_Origins_Significance_and_Global_Trajectories

164. Greenleaf (2014). https://www.researchgate.net/publication/272236641_Sheherezade_and_the_101_Data_Privacy_Laws_Origins_Significance_and_Global_Trajectories

165. Case C-311/18: Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems.

166. Court of Justice of the European Union (2020). PRESS RELEASE No 123/20, Luxembourg, 6 October 2020.

167. Greenleaf (2019). https://it.scribd.com/document/411861387/Global-data-privacy-laws-2019

168. International Association of Privacy Professionals (2018). IAPP, FTC, OPC, PCPD collaborate on connected-toy enforcement. Jan 9, 2018. https://iapp.org/news/a/ftc-settles-first-case-involving-connected-toys/

169. Carson, A. (2019). DPAs from DPC stage: Fines don't mean everything. IAPP November 20, 2019.

170. Bracy, J. (2020). DPAs talk priorities at IAPP Europe DPI: France. IAPP 2020.

171. Buttarelli (2019). https://iapp.org/resources/article/privacy-2030/

172. IEEE Standards website: https://www.ieee.org/standards/index.html

173. Feldstein, S. (2020). State surveillance and implications for children, UNICEF Good Governance of Children's Data project. Issue brief no. 1. August 2020. https://www.unicef.org/globalinsight/reports/state-surveillance-and-implications-children

174. Hartung (2020). https://www.unicef.org/globalinsight/reports/childrens-rights-design-new-standard-data-use-tech-companies

175. Hartung (2020). https://www.unicef.org/globalinsight/reports/childrens-rights-design-new-standard-data-use-tech-companies

176. Hartung (2020). https://www.unicef.org/globalinsight/reports/childrens-rights-design-new-standard-data-use-tech-companies

177. United Nations (2021). Big data and artificial intelligence. https://www.unglobalpulse.org/

178. Information Commissioner's Office (ND). How does the right to erasure apply to children? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/how-does-the-right-to-erasure-apply-to-children/

179. Dignum, V. et al. (2020). Policy Guidaance on AI for Children, UNICEF New York. https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf

180. Perry, A.M., and Lee, N.T. (2019). AI is coming to schools, and if we're not careful, so will its biases. Brookings Institution.

181. Benevolent (2019). Mind the Gap: The Diversity Issue In Medical Research. October 6, 2019. https://www.benevolent.com/news/mind-the-gap-the-diversity-issue-in-medical-research

182. Cooper, D. et al. (2020). The European Commission publishes a proposal for a Regulation on European Data Governance (the Data Governance Act). Inside Privacy. https://www.insideprivacy.com/data/the-european-commission-publishes-a-proposal-for-a-regulation-on-european-data-governance-the-data-governance-act/

183. Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) COM/2020/767 final

184. Buttarelli (2019). https://iapp.org/resources/article/privacy-2030/ Buttarelli (2019). https://iapp.org/resources/article/privacy-2030/ Buttarelli (2019). https://iapp.org/resources/article/privacy-2030/

185. Global Commission on Internet Governance, Who Runs the Internet? The Global Multi-Stakeholder Model of Internet Governance, 2016.

186. Verhulst, S. (ND). A Distributed Model of Internet Governance, Global Partners Digital.

187. Lovett, R., L., V., Kukutai, T., Cormack, D. C., Rainie, S. and Walker, J. (ND). Good Data Practices for Indigenous Data Sovereignty and Governance.

188. Johnson, K. (2020). Amsterdam and Helsinki launch algorithm registries to bring transparency to public deployments of AI. Venturebeat. September 28, 2020.

189. Draft Recommendation of the OECD on Children in the Digital Environment.

190. Hogan Lovells (2021). Children's rights in the digital world: new guidelines in the Netherlands. Engage Legal Insights and analysis. 17 March 2021. https://www.engage.hoganlovells.com/knowledgeservices/news/childrens-rights-in-the-digital-world-new-guidelines-in-the-netherlands

191. Hartung (2020). https://www.unicef.org/globalinsight/reports/childrens-rights-design-new-standard-data-use-tech-companies

192. 5Rights Foundation & Digital Futures Commission (2021). Child Rights Impact Assessment: A tool to realise children's rights in the digital environment. https://digitalfuturescommission.org.uk/wp-content/uploads/2021/03/CRIA-Report.pdf

193. Information Commissioner's Office (2020). Children's privacy and data sharing in focus as ICO regulatory sandbox re-opens. ICO news release 11 Sep 2020.

194. Information Commissioner's Office (2021). Current Projects. https://ico.org.uk/for-organisations/current-projects/#yoti-doc-scan

195. Deloitte (2018). A journey through the FCA regulatory sandbox. The benefits, challenges, and next steps. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-fca-regulatory-sandbox-project-innovate-finance-journey.pdf

196. Federman, H. (2021), Moving beyond notice and choice to welcome a fiduciary standard. IAPP.

197. Open Data Institute Blog (2020). Data trusts in 2020, Open Data Institute. https://theodi.org/article/data-trusts-in-2020/.

198. Open Data Institute Blog (2020). https://theodi.org/article/data-trusts-in-2020/

199. European Commission (2020). Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN

200. MyData Global. https://mydata.org

201. Heseleva et. al. (2020). Towards a Multilateral Consensus on Data Governance, G20 Insights. https://www.g20-insights.org/policy_briefs/towards-a-multilateral-consensus-on-data-governance/

202. Mhlambi, S. (2020). "From Rationality to Relationality: Ubuntu as an Ethical & Human Rights Framework for Artificial Intelligence Governance", *Carr Center Discussion Paper, Harvard Kennedey* School, Harvard University. https://carrcenter.hks.harvard.edu/publications/rationality-relationality-ubuntu-ethical-and-human-rights-framework-artificial

203. Mhlambi, S., Freuler Ortiz, J. and Ricaurte, P. (2019). Think South: Reimagining the Internet. https://cyber.harvard.edu/story/2019-10/think-south-reimagining-internet

204. Lovett, Kukutai, Cormack, Rainie and Walker (ND). https://static1.squarespace.com/static/5b3043afb40b9d20411f3512/t/5b70e9c889858355258ae64a/1534126543958Good+data+practices+for+Indigenous+Data+Sovereignty+and+Governance+submitted.pdf

205. Mhlambi (2019). https://cyber.harvard.edu/story/2019-10/think-south-reimagining-internet

206. Mhlambi (2019). https://cyber.harvard.edu/story/2019-10/think-south-reimagining-internet

UNICEF works in the world's toughest places to reach the most disadvantaged children and adolescents — and to protect the rights of every child, everywhere. Across 190 countries and territories, we do whatever it takes to help children survive, thrive and fulfill their potential, from early childhood through adolescence. And we never give up.

The Office of Global Insight and Policy serves as UNICEF's internal think-tank, investigating issues with implications for children, equipping the organization to more effectively shape the global discourse, and preparing it for the future by scanning the horizon for frontier issues and ways of working. With dedicated expertise in seven policy areas — digital technology, human capital, governance, the environment, society, markets, and finance — the Global Insight team assists the organization in interpreting, and engaging in, a rapidly changing world.

Office of Global Insight and Policy

United Nations Children's Fund

3 United Nations Plaza, New York, NY, 10017, USA

Cover photo: ©UNICEF/UN0139511/Gilbertson VII Photo