COVID-19: A spotlight on child data governance gaps

Linda Raftree, independent consultant, Emma Day, independent consultant, and Jasmina Byrne, UNICEF

Even before the COVID-19 pandemic, the world was hurtling down a path of rapid growth in technology, with the convergence of ground-breaking innovations such as the internet of things; artificial intelligence (AI) systems and machine learning; biotechnology; robotics; and virtual reality. New technologies offer great promise to improve many areas of children’s lives, giving them unparalleled access to information and learning tools, propelling breakthroughs in paediatrics, and supporting the work of those who provide health, education, and social services. These new technologies share one feature — they rely on massive amounts of data. Their success is generally proportional to the amount of data they are able to collect, including data from children. With a few exceptions, that data comes from constant collection, tracking, and analysis of human behaviour, which in turn gives more power to the data gatherers, enabling them to influence our current and future behaviour.

Since the COVID-19 pandemic took hold, technology has assumed an even more prominent role in children’s lives. Data-powered technology has been used — with varying degrees of success — to track, trace, and control the novel coronavirus infection rate, as well as to continue the remote provision of education, health, and social services to children while cities and countries have locked down.

Urgency has concentrated on bringing necessary services to children, and less attention has been paid to privacy and protection of data. The general public, including children, cannot see or immediately comprehend how these data systems work and connect with one another. This is largely due to the fact that transparent and accountable data management frameworks are often not put in place prior to the deployment of these technologies. In addition, governments generally lack the kind of clear, technical, and evidence-based orientation that would ensure children gain maximum and equitable access to the benefits of new technologies while remaining protected from privacy infringements.

Given the human rights implications of collecting information on and closely tracking the behaviour of the public, it has become all the more urgent to limit inappropriate and/or potentially harmful uses of data,
including that of children. Data from and about children present unique challenges that stem from their vulnerability, fluidity of their attitudes, preferences and identity, and the initially low capacity to exhibit full agency and to make informed decisions. In this brief we offer a glimpse into challenges related to the protection of children’s data during the COVID-19 pandemic and highlight some key policy issues that need to be addressed. Some of these challenges are not new and will continue into the foreseeable future, unless we collectively articulate better that the world we want for children is one where their rights are respected, data about them is safeguarded and is not exploited for commercial and other purposes.

In which situations can children’s data and privacy be compromised?

By the end of August 2020, more than 23 million COVID-19 infections and over 800,000 deaths had been confirmed in 188 countries and territories. As early as April 2020, at least 84 countries had declared public emergencies, encouraged national lockdowns, or suspended citizen rights in some way because of COVID-19. This, combined with weak or non-existent privacy laws in many countries, has opened up the possibility of what has been described as “the most massive personal data grab that’s ever occurred.” Children’s data is included in the huge amount of data being captured. Children now spend more time online or are being offered services that require use of digital technologies, thus generating more digital data which is often shared on platforms with insufficient data protection safeguards. Yet their privacy rights are conspicuously absent from current debates related to public health and risks to privacy. Children are surveilled by governments and the private sector alike when they access online health, education and other services, and when they use the internet for socialisation, play, and entertainment.

Furthermore, in the rush to address pandemic challenges, urgency has concentrated on bringing necessary services to children, and less attention has been paid to privacy and protection of data. In some cases, this is because of the need for quick action. In other cases, it is because emergency laws have allowed for a loosening of data protection regulations which led to amassing greater amounts of data in ways that will be difficult to roll back in the future.

Due to lockdown and social distancing taking place in the majority of countries, schools, health-care providers, social welfare and child protection agencies, and many community organizations report that they have restricted their programming and services or are managing them remotely by mobile phone or online. When commercial platforms that were not designed for protection and the exchange of highly sensitive data are used by health professionals, educators, therapists, and social workers, there are risks that children’s personal data will be collected and used by these platforms for purposes such as targeted marketing, profiling, and predictive analytics related to health or education. Some situations where children’s data warrant special consideration are summarized below.

Children are surveilled by governments and the private sector alike when they access online health, education and other services.

Online platforms, applications, social media and data protection

Children are accessing the internet at younger and younger ages. With the COVID-19 pandemic, parents who are balancing working from home and childcare are allowing their children more time with their digital devices, and much of that time is spent on platforms that capture their data. In the United States, for example, a study found that 76 per cent of parents had relaxed “screen time” rules. Children’s play and social lives are moving online as well, and there are indications that younger children are using social media and social networking tools that are not designed for them. In addition to going online to access education and other services, children in many parts of the world are spending more time online to connect with friends or to keep themselves entertained on social media or to play online games. The average time per day spent on social media apps by American children aged between 4 and 15 years old almost doubled in 2020 compared to 2019.

Social media and search engines regularly collect data on children based on their registration and login details, online activities (browsing history, communication, content interaction), content cre-
ation (emails, photos, videos) and device data (IP address, device IDs, unique identifiers). Increased online engagement by children leads to a higher volume of data collected by companies and data brokers, and the potential for inappropriate collection, use, and sharing of children's data multiplies. These platforms and networks might link children's data together in harmful ways now or in the future, exposing them to profiling and targeted marketing for products, services, and content not meant for their age group.

For example, marketers and advertisers have already begun using their troves of data to “COVID-wash” their activities and re-package them as useful news about the virus, for example by creating maps of where people are traveling immediately after localised COVID-19 outbreaks, and using mobile phone-based location tracking to predict which places might be safer or more dangerous. Advertisers are using social media data about individuals to target them with ads that prey on people's emotional vulnerability and promote specific products, for example, cigarettes and tobacco. Advertising technology has introduced a new generation of tracking and targeting software systems that make it possible to access, analyze, and act upon a wealth of data on individual consumers, including purchasing behaviour, device use, social media communications, online interests, location and geographic movements, financial status, health concerns, and much more.

Children are not sufficiently protected from these practices, which can put them at risk of commercial exploitation and influence their opinions and behaviour in ways not always healthy for their growth and development. As commerce is now being driven online due to the closure of brick and mortar stores, advertisers are likely to collect more data to track market changes and identify new opportunities to target children and their parents who are now a captive audience at home.

Advertisers are likely to collect more data to track market changes and identify new opportunities to target children and their parents who are now a captive audience at home.

Health technology and public health surveillance

In the health sector, prior to COVID-19, the use of new technologies in paediatrics had expanded, and data had enabled the development of personalised medicine, designed to respond to the needs of the patient at an individual level and allowing for data-enabled assessment, diagnoses, and treatments. Data is also used to help determine predispositions to disease and to design targeted prevention strategies, as well as to provide a powerful tool for predicting the spread of pandemics. Digital health interventions for children have demonstrated impacts on a wide range of outcomes, including quality of care and information, reducing supply stock-outs, and improving adherence to treatment regimes.

Technology has also been harnessed to combat COVID-19 in a myriad of ways, including genetic sequencing, vaccine development, and prediction and tracking of outbreaks and hotspots. A high-profile use of technology for COVID-19 which caught the attention of the public, governments, and the private sector was contact tracing apps. These were trialled around the world with varying degrees of success and failure. Digital contact tracing prompted heated debates about privacy and surveillance given that sensitive health data can be linked to identifiable personal and location data in order to track, test, and isolate anyone who comes into contact with another person who has been confirmed to have the virus. Contact tracing apps collect population-wide data, including from children, yet there has been little or no mention of children's special privacy rights. Where legal frameworks do exist, such as in Articles 6 and 9 of the European Union's General Data Protection Regulation (GDPR), they may provide an exception for data confidentiality rules when the data is related to prevention of a public health crisis, with a caveat that any limitations to privacy protections must be proportionate. But as many governments declared a state of emergency related to COVID-19, normal data privacy rules did not always apply.

If contact tracing or other apps that collect this type of widespread personal and/or sensitive data are to be considered a proportionate limitation of the public's privacy rights, then they must first be proven necessary and effective in combating the virus. While traditional contact tracing has greatly con-
tributed to overcoming previous, highly contagious pandemics, there has been little proof of the necessity and effectiveness of the types of digital contact tracing applications that were launched during the first phases of the COVID-19 crisis.\textsuperscript{21,22} Some reports have reflected considerable scepticism regarding the contribution of contact tracing apps in limiting the spread of the virus, as opposed to the impact of other measures such as widespread testing, mandatory mask wearing, strict and early lockdown, and restriction of movement.\textsuperscript{23}

When contact tracing is done through a mobile application, unless clear regulation is in place to control the collection, use, and sharing of data, it can easily be linked with other personal data collected by companies, such as advertising and product data, or data from social media activities. Unless regulation stipulates how long this information can be retained and stored, there are risks of reuse of such sensitive information in unexpected or exploitative ways.\textsuperscript{24} Algorithmic bias in software used by healthcare services can be especially dangerous because children lack the awareness or resources necessary to rectify bias or inaccuracies in their data. When personal data is mishandled, children and families may lose trust in institutions that deliver essential health services such as vaccines, medicine, and nutrition supplies.\textsuperscript{25}

The rapid move to telemedicine has given rise to concerns about data privacy and security.\textsuperscript{26} Since the outbreak of COVID-19, telemedicine is being widely adopted in both rich and poor countries in response to physical distancing protocols. The rapid move to telemedicine, however, has given rise to concerns about data privacy and security, especially in cases where privacy protocols are not well established or telemedicine (including mental health counselling) is happening over platforms that were not designed for this purpose. Chatbots, for example, are being tested as a first point of contact for patients in some African countries.\textsuperscript{26} In refugee camps, some frontline workers have reported having to manage medical triage for children in refugee camps using channels such as WhatsApp or Zoom, which has raised concerns related to data privacy and protection.\textsuperscript{27}

Laws regulating how health data can be shared do not necessarily cover the provision of health and mental health services over new platforms that collect back-end and a variety of other data, and which potentially link sensitive health information with personal data.\textsuperscript{28,29} When breaches happen in a telehealth context, extremely sensitive data can be revealed. A major telehealth provider in the UK suffered a breach in 2020 that allowed its 2.3 million registered users to access videos of other patients’ appointments with their doctor. One patient was able to view around 50 patient consultations as a result of the security failure.\textsuperscript{30}

Distance/remote education and children’s data

Since the COVID-19 pandemic started, some 1.4 billion learners in 143 countries have been affected by school closures.\textsuperscript{21} In an effort to continue with education during the pandemic, schools around the world are turning to technology-enabled remote learning for children under lockdown. While digital education has provided essential links to learning, teachers, and peers, it has its own challenges in terms of data governance. These predate COVID-19 but have now become more apparent.

In 2019, a US non-profit organization evaluated educational technology (EdTech) tools and found that only 20 per cent of the applications and services reviewed met minimum safeguarding standards.\textsuperscript{32} Gaps include: corporate tracking of student activities both inside and outside the classroom, discrimination against children and young people from historically marginalized groups, ongoing monitoring of activities leading to a loss of student autonomy, and the sale of student data to third parties who often use it for advertising.\textsuperscript{33}

Platforms being incorporated into the remote education toolbox include Zoom, Skype in the Classroom, Google Classroom, Facebook and many others. Some of these platforms have been called out by data protection professionals for their potential data security flaws and privacy issues. Often the only consent needed for incorporating these as mandatory tools for education is that of a school official or teacher, raising the question of whether schools can consent to data collection by these platforms on behalf of students and their caretakers.

Children are required to use the platforms in order to access education, meaning that true consent is not possible — they must provide their personal data in
exchange for accessing their fundamental right to education. This also places the burden of determining the acceptability of a platform or application's data protection and privacy policies on educators and school systems. Teachers and school administrations do not normally have the knowledge, time, or capacity to review terms and conditions and platform privacy policies, and the COVID-19 pandemic has only exacerbated this challenge.

Many countries have legislation that governs health data. Education data, which is often just as sensitive, is less protected in data privacy laws. This means that even in countries where the rule of law is strong, it might be difficult to hold EdTech service providers accountable for the ways that they use and/or share children's data. Because the use of technology in education systems is likely to continue post-pandemic, choices about EdTech need to be made conscientiously with close attention to how children's data is protected now and in the future. Policy makers should support teachers, administrators, and school boards to better understand and manage online educational tools and protect children from exploitative or harmful uses of their data.

Online child welfare services and data protection

Countries where quarantine is strict have seen social services go into lockdown as well. In some parts of the United States, for example, cases that would normally involve home visits have temporarily moved online. Non-governmental and community-based organizations have reported that protection and gender-based violence services have been disrupted or have had to move online in order to ensure the health and safety of frontline professionals and comply with lockdown mandates. It also means that some visits that would ordinarily be documented on paper or on devices provided by an organization are being made virtually on staff personal devices, meaning that contacts and data stored on these devices might be accessible to other family members who use the same device. Storage and transmission of data might also be less secure on home-based networks or might be transmitted via platforms that are not protected by end-to-end encryption. Staff may not have the necessary security training, and documentation of visits might not be conducted in ways that protect the privacy and security of children's most personal and sensitive information. This includes data collected on paper, which might not be stored as securely in the home as it would be in an office. Moreover, when in lockdown, children might not have a private place from which to speak with child welfare professionals.

Child helplines form an important part of national child protection systems. Usually calls are tracked and children's personal information is recorded in a database. Data is not yet available to give the full picture of the impact of COVID-19 on child helplines, although in the EU there was a significant increase in calls in the first quarter of 2020, before the lockdown. The WHO reported a spike in calls to helplines by both children experiencing violence against themselves and women experiencing domestic violence. Due to quarantine, many children are cut off from the people in their lives they may ordinarily have turned to for help, and in accessing support via helplines more data is likely to be collected about them and stored online.

Children are required to use the platforms in order to access education, meaning that true consent is not possible.

Child helplines often partner with private telecoms providers who offer the phone platform and sometimes assist with storing and processing the data related to children's calls. Without clear and comprehensive legal agreements between child helplines and the telecoms providers there can be little clarity and accountability regarding aspects such as how any data related to children is collected, stored and used, who owns the right to that data in accordance with international and national laws, and how potential problematic secondary uses of children's data is controlled for and prevented. Therefore, it is paramount that where helplines are set up or expanded to respond to emergencies such as COVID-19, they have legal agreements in place with telecoms providers to ensure that all data collected from children is kept securely, for a limited period of time, and that sharing or use of the data is not permitted beyond the specified purposes.

Considerations for good governance of children's data

As reactions to COVID-19 move from the acute emergency phase into a “new normal,” excuses for
overcollection of data with little oversight will fall flat. Now is the time for governments to act quickly and offer better protection of children’s data rights. They could start by reviewing their laws and policies and developing frameworks and guidelines for ethical use and safeguards of children’s data during emergency situations, including during future pandemics. These should be integrated into government regulations, terms and conditions of EdTech products, health products, contact tracing apps, and other products children are likely to use or benefit from. Term limits, also referred to as “sunset clauses,” need to be established for any emergency data collection permissions so that protections are put back in place once the emergency ends or becomes manageable. As outlined in the Responsible Data for Children principles, the collection and use of children’s data must be purpose-driven, proportional, professionally accountable, people-centric, participatory, protective of children’s rights, and prevent harm across the data cycle.42

The situations mentioned above represent only some of the potential challenges regarding fair, ethical and transparent collection and use of children’s data. The data uses and practices discussed here are not clear-cut cases and therefore require the balance between public good and data protection to be weighed carefully. They also require an understanding of emerging practices, potential future data use and careful consideration for individual and group data rights. Above all, children’s needs and their best interests must guide all the decisions about the use of their data now and in the future.
**Good Governance of Children’s Data project**

The Office of Global Insight and Policy is bringing together 17 global experts in a project 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. Debate on the future of children’s data affects a diverse range of issues, including data ownership and control, data fiduciaries, profiling for digital marketing purposes, child-friendly privacy notices, data erasure upon request, age verification, parental responsibility, data protection by design and default, algorithmic bias, and individual and group data.

The project aims to highlight the gap between the world we want for children and today’s reality, developing a manifesto on how children’s data could be optimally managed and what steps need to be taken. To help develop this manifesto, members of the working group will publish short analyses of different approaches to data governance.

**Endnotes**

4. Aljazeera (2020) Coronavirus: Which countries have confirmed cases?
9. Marketing Charts (July 2020). TikTok Engagement Among Kids Surges During the Pandemic.
11. UNICEF (2020) Coronavirus Disease (COVID-19) and Its Implications for Protecting Children Online: A technical note from UNICEF and partners.
16. Ibid.
18. UNICEF’s Approach to Digital Health (n.d.), UNICEF Health Section Implementation Research and Delivery Science Unit and the Office of Global Innovation.
As part of a separate research project by one of this paper’s authors, a series of interviews on the topic of COVID-19 and data protection was conducted with frontline staff in five countries.


British Association for Counselling and Psychotherapy (2020). Working Online with Children and Young People: Guidance for members, 10 July 2020.


UNESCO (2020). Education: From disruption to recovery.


This point was raised in interviews with frontline staff during a research project being conducted by one of this paper’s authors.


For programme delivery and services by practitioners see Responsible Data for Children Principles and Child Helpline International Quality Standards for Child Helplines, Principle 9.4: Data Protection.


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

© United Nations Children’s Fund (UNICEF), August 2020

The authors are grateful to Lindsey Barrett, Caroline Cinders, Steven Vosloo, Gabrielle Berman and Karen Carter for their thoughtful comments and input into the text.

This is a working document. It has been prepared to facilitate the exchange of knowledge and to stimulate discussion. The text has not been edited to official publication standards and UNICEF accepts no responsibility for errors. The statements in this publication are the views of the author(s) and do not necessarily reflect the policies or the views of UNICEF. The designations in this publication do not imply an opinion on legal status of any country or territory, or of its authorities, or the delimitation of frontiers.