unicef
Office of Research – Innocenti

Covid-19 & Children

Digital contact tracing and surveillance during COVID-19

General and Child-specific Ethical Issues

Gabrielle Berman, Karen Carter, Manuel García-Herranz
and Vedran Sekara

Office of Research – Innocenti Working Paper
WP 2020-01 | June 2020

unicef | for every child

UNICEF OFFICE OF RESEARCH – INNOCENTI

The Office of Research – Innocenti is UNICEF's dedicated research centre. It undertakes research on emerging or current issues in order to inform the strategic direction, policies and programmes of UNICEF and its partners, shape global debates on child rights and development, and inform the global research and policy agenda for all children, and particularly for the most vulnerable.

Office of Research – Innocenti publications are contributions to a global debate on children and may not necessarily reflect UNICEF policies or approaches.

The Office of Research – Innocenti receives financial support from the Government of Italy, while funding for specific projects is also provided by other governments, international institutions and private sources, including UNICEF National Committees.

INNOCENTI WORKING PAPERS

UNICEF Office of Research Working Papers are intended to disseminate initial research contributions within the programme of work, addressing social, economic and institutional aspects of the realization of the human rights of children.

The findings, interpretations and conclusions expressed in this paper are those of the authors and do not necessarily reflect the policies or views of UNICEF.

The authors declare that there were no conflicts of interest in the production of this working paper.

This paper has been peer reviewed both externally and within UNICEF.

The text has not been edited to official publications standards and UNICEF accepts no responsibility for errors.

For readers wishing to cite this document, we suggest the following form:
Berman, G., Carter, K., García-Herranz, M. and Sekara, V. (2020). Digital contact tracing and surveillance during COVID-19 - General and Child-specific Ethical Issues, Innocenti Working Paper 2020-01, UNICEF Office of Research – Innocenti, Florence.

DIGITAL CONTACT TRACING AND SURVEILLANCE DURING COVID-19

GENERAL AND CHILD-SPECIFIC ETHICAL ISSUES

Gabrielle Berman[i]

Karen Carter[ii]

Manuel García-Herranz[iii]

Vedran Sekara[iv]

[i] UNICEF Office of Research – Innocenti
[ii] UNICEF Data and Analytics Section
[iii] UNICEF Office of Innovation
[iv] Independent Consultant, UNICEF

> "While we understand and support the need for active efforts to confront the pandemic, it is also crucial that such tools be limited in use, both in terms of purpose and time, and that individual rights to privacy, non-discrimination, the protection of journalistic sources and other freedoms be rigorously protected. States must also protect the personal information of patients. We strongly urge that any use of such technology abide by the strictest protections and only be available according to domestic law that is consistent with international human rights standards."[1]
>
> – Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

This working paper was reviewed and strengthened by the inputs of Sigrun Kaland (UNICEF Office of the Executive Director), Remy Mwamba, Karin Källander and Elevanie Nyankesha (UNICEF Health Section), Tyler Porth (UNICEF Data and Analytics Section) and Steven Vosloo (UNICEF Office of Global Insight and Policy).

[1] Statement by Mr David Kaye, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; Mr Harlem Désir, Organization for Security and Co-operation in Europe Representative on Freedom of the Media; and Mr Edison Lanza, Inter-American Commission on Human Rights Special Rapporteur for Freedom of Expression, 19 March 2020. Available at: Office of the High Commissioner for Human Rights, 'COVID-19: Governments muct promote access to and free flow of information during pandemic – International experts', Geneva/Washington/Vienna, 19 March 2020, <www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=25729&LangID=E>, accessed 25 May 2020.

TABLE OF CONTENTS

INTRODUCTION

The last few years have seen a proliferation of means and approaches being used to collect sensitive or identifiable data on children. Technologies such as facial recognition and other biometrics, increased processing capacity for 'big data' analysis and data linkage, and the roll-out of mobile and internet services and access have substantially changed the nature of data collection, analysis and use.

Real-time data are essential to support decision-makers in government, development and humanitarian agencies such as UNICEF to better understand the issues facing children, plan appropriate action, monitor progress and ensure that no one is left behind. But the collation and use of personally identifiable data may also pose significant risks to children's rights.

UNICEF has undertaken substantial work to provide a foundation to understand and balance the potential benefits and risks to children of data collection. This work includes the Industry Toolkit on Children's Online Privacy and Freedom of Expression[2] and a partnership with GovLab on Responsible Data for Children (RD4C) – which promotes good practice principles and has developed practical tools to assist field offices, partners and governments to make responsible data management decisions –

Balancing the need to collect data to support good decision-making versus the need to protect children from harm created through the collection of the data has never been more challenging than in the context of the global COVID-19 pandemic. The response to the pandemic has seen an unprecedented rapid scaling up of technologies to support digital contact tracing and surveillance. The initial approach has included:

- tracking using mobile phones and other digital devices (tablet computers, the Internet of Things, etc.)
- surveillance to support movement restrictions, including through the use of location monitoring and facial recognition
- a shift from in-person service provision and routine data collection to the use of remote or online platforms (including new processes for identity verification)
- an increased focus on big data analysis and predictive modelling to fill data gaps.

As the pandemic progresses, we are also likely to see the emergence of more applications that link datasets as we seek to better understand the secondary impacts of the pandemic on children and their families. This has implications for privacy as the linking of datasets: increases the likelihood that children will be identifiable; increases the opportunity for (sensitive) data profiling; and frequently involves making data available to a broader set of users or data managers. It is recognized that reuse of unidentifiable data could potentially serve future public health responses and research. But the nature of, access to and use of the data now and in future necessitate accountability, transparency and clear governance processes should be in place from the outset These are needed to ensure that data privacy is protected to the greatest degree possible and that the limitations to the use of these data are clearly articulated. These issues will be explored throughout this working paper.

[2] Nyst, C., Gorostiaga, A., and P. Geary (2018) Industry toolkit on Children's online privacy and freedom of expression the Industry Toolkit on Children's Online Privacy and Freedom of Expression, https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf

Methodology

The following is a 'light touch' review of the literature and other sources, which attempts to provide a broad overview of the ethical issues presented by the use of various digital technologies for contact tracing and surveillance for public health purposes. The literature was primarily sourced from public analysis and grey literature, with academic literature included wherever possible. Unfortunately, given the relatively contemporary nature of the use of these digital technologies for public health purposes, the evidence base is limited. This working paper therefore attempts to unpack the critical issues in the use of these technologies in light of their recent proliferation and adoption, while recognizing that the evidence needed to fully understand the efficacy of such approaches in different contexts is limited.

Who is involved?

The recent use of digital technologies for public health surveillance has resulted in a significant shift in the governance of data collection processes. As is the case for traditional public health surveillance, many of these initiatives have been sponsored or managed by government. This is the case in India (Aarogya Setu via Bluetooth), the Islamic Republic of Iran, Israel, Poland, the Republic of Korea, Singapore (TraceTogether) and the Russian Federation (facial recognition). Private companies and research institutions are also very much at the forefront of both contact tracing and surveillance applications. The various applications that have been developed by both private corporations and research institutions and which are currently being used include:

- Google COVID-19 Community Mobility Reports, which show aggregate information related to movement and congregations of people to determine whether work-from-home arrangements are minimizing congregations
- Private Kit: Safe Paths, a location-tracing application developed by Massachusetts Institute of Technology, which uses a smartphone's Global Positioning System (GPS) location
- an application co-designed by Apple and Google that warns individuals if they have been in contact with someone who has tested positive for the disease
- an application called DP-3T (Decentralized Privacy-Preserving Proximity Tracing), which has been built on top of the Apple/Google application program interface and is now endorsed by almost 600 academics[3]
- PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing), a software system that is intended to support European countries to deliver their own contact-tracing applications.

Other private firms that provide biometric systems to governments are also purportedly working with government agencies to track the spread of COVID-19 and assess how hospitals are dealing with increases in identified cases.

These examples highlight both the changing role of private industry and academia in meeting a public demand for data, and the increasing role of public-private partnerships in collecting, managing and using data on individuals for the 'public good'.

[3] An application programme interface (API) comprises routines, protocols and tools, and is used to build software applications.

Alongside the rapid development of new applications, and changes to existing data systems, we have also seen a number of countries relaxing existing safeguards for data protection or setting them aside altogether. Examples range from allowing doctors to use personal (unprotected) phones for telehealth consultations to the relaxing of regulations on the use of mobile phone data to the passing of a bill that allows surveillance inside homes_of people placed under quarantine.

It is imperative that we do not lose sight of children's rights in this challenging environment. The speed at which the data environment is changing and the evolving nature of 'who' is able to access, use or make decisions about individuals' data calls for broad engagement with all key players in this space. The rights to privacy and to be protected from harm are enshrined in the United Nations Convention on the Rights of the Child[4] and should not be set aside even as we support the best possible use of data to monitor and, we hope, mitigate the impacts of the current COVID-19 pandemic.

WHAT TECHNOLOGIES AND DIGITAL DATASETS ARE BEING USED?

As noted prevously, a number of technologies are being adopted to address the need for contact tracing and surveillance and to better understand the nature of the COVID-19 pandemic. These include mobile phone tracking, biometric technologies and data scraping, each of which is unpacked below. These technologies may be used in addition to more traditional manual contact tracing and surveillance approaches.

Mobile phone tracking: Mobile phones and mobile data are one of the key sources of information being adopted for digital contact tracing. In some instances, mobile phone tracking requires the voluntary download of a contact-tracing application (including giving consent to share individual information with the database). In other instances, governments are strongly urging or requiring populations to use such applications.

Mobile phones are also being used for surveillance, with location data from mobile network operators used to determine whether and where people are congregating and whether social distancing measures are working.

Biometric technologies: These technologies use unique and permanent physical traits or characteristics such as face shape or fingerprints to identify an individual. When the individual is enrolled in the system – for example, a national identification system – the biometric trait is captured and converted to a digital template to be stored in the system for future reference. Matching involves using an algorithm to assess the similarity between the reference template and a new image captured by a sensor. Matching can be carried out either against a group of records to identify a 'person of interest' (such as in active street camera surveillance) or against a specific record to verify that an individual is indeed who she/he claims to be (such as when verifying a cash payment against an intended recipient).[5] While a range of biometric traits can be used for identification and verification, facial recognition is the most widespread and relevant technology for contact tracing and public health surveillance. Accuracy of the matching is affected by the quality of the camera, the age of the individual it is being used to identify,

[4] The United Nations., *Convention on the Rights of the Child*, Treaty Series 1577 (November): 3., 1989.

[5] Du, Eliza, ed., *Biometrics: From fiction to practice*, Pan Stanford, Singapore, 2013.

environmental conditions, the trait itself and biases in the algorithm, among many other factors. The permanent nature of biometric identifiers makes these particularly sensitive identifiable data.[6]

Data scraping/collation (artificial intelligence): Data are also being mined from social media posts for mentions of specific symptoms to predict the spread of the disease (surveillance).

To understand the concerns that have been raised, a number of issues need to be understood in relation to the technology.

GETTING TO THE HEART OF THE ISSUE: HOW DIGITAL DATA ARE COLLECTED AND STORED FOR CONTACT TRACING AND SURVEILLANCE

There are two primary forms of tracing:

- digital proximity tracing
- location tracing.

Digital proximity tracing

Digital proximity tracing aims to provide information about whether an individual has been near someone who has the virus (contact tracing).

For proximity tracing, while geographical location data may be collected, these need not be shared with potential contacts.[7] Proximity tracing recognizes that the transmission of a pathogen occurs through close proximity. Therefore, the only data necessary to determine a potential exposure through close proximity transmission are data that confirm both:

a) an instance of physical proximity to an infected person for a sufficient period of time

b) that this exposure took place during a period of time when transmission from the infected person could have occurred, i.e., the infected person was in the contagious phase of the illness.

No additional information about the infected person, her/his other contacts, the location of the encounter, the context of the encounter, or any other factors is necessary.[8]

[6] For a greater understanding of biometric technologies and the general risks and benefits of their use with children, see: United Nations Children's Fund, *Faces, Fingerprints and Feet: Guidance on assessing the value of including biometric technologies in UNICEF-supported programs*, UNICEF, July 2019, available at: <www.data.unicef.org/biometrics>, accessed 25 May 2020.

[7] European Data Protection Board, *Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak, Adopted on 21 April 2020*, EDPB, 2020. Available at: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf>, accessed 25 May 2020.

[8] Salathé, Marcel, and Ciro Cattuto, 'COVID-19 Response: What data is necessary for digital proximity tracing?', 2020. Available at: <https://github.com/DP-3T/documents/blob/master/COVID19%20Response%20-%20What%20Data%20Is%20Necessary%20For%20Digital%20Proximity%20Tracing.pdf>, accessed 25 May 2020.

When used widely within the population (applications based on both Bluetooth and GPS technologies are capable of determining whether someone with COVID-19 has crossed another individual's path. This can only occur when positive cases are registered and indicated as such by the affected individual. It should be noted that Bluetooth data are more reliable for tracing person-to-person contact, as GPS coordinates are defined within a specific space, e.g., a building.[9] Further, Bluetooth data, once anonymized, are less vulnerable to de-anonymization than location histories from GPS data.

Storing the data

How the data are stored and by whom is critical when considering privacy. There are two forms of storage – decentralized and centralized storage.

Decentralized storage: Information can be collected and stored in the individual's personal phone. Privacy considerations such as maintenance of data control by the data subject are achievable through decentralized processes or hybrid approaches, as these avoid the sharing and processing of personal data through centralized collection points.

Centralized storage: Information can be collected from individuals and stored centrally by government, private institutions or organizations, or public institutions such as hospitals. Centralized approaches are used to implement biometric technologies such as facial recognition, or for collection and analysis of individual GPS data at a centralized location. It should be noted that centralized approaches have significant privacy implications and are unnecessary to meet the data requirements for digital proximity tracing.

Limitations of contact-tracing technologies

There are a number of limitations to contact-tracing technologies. While largely non-resource-intensive, contact tracing – like other digital technologies – is open to fraud and abuse, according to the basic limitations of the technologies themselves. Limitations include the following:

- **An inability to account for other factors, usually included in manual tracing,** that are specific to the environment, such as wind direction or presence of ventilation.
- **GPS and Bluetooth technologies may be able to determine proximity but cannot establish safety per se**, given that barriers between people, such as walls or windows, will not automatically be factored into risk profiles when using Bluetooth data, or people may be spatially distanced but occupy the same GPS coordinate, as noted above.
- **Dependence on self-enrolment and downloading of the application.** This not only requires trust in the government and the platform, but also a belief in the value and importance of contact tracing. As researchers have noted, the high level of uptake required for contact tracing to be effective in suppressing COVID-19 is unrealistic in many countries.[10]
- **Dependence on self-isolation.** Where individuals retain their own data and/or are anonymous, they must be prepared to self-isolate when notified of contact with someone with the virus. If not, the contact-tracing process is ineffectual.

[9] For example, an individual could be at the same GPS coordinate as an infected person but situated 10 floors above that infected person.

[10] Hinch, Robert, et al., *Effective Configurations of a Digital Contact Tracing App: A report to NHSX*, University of Oxford, Oxford, 2020.

- **An inability to capture asymptomatic carriers**, who are unaware that they are infected.
- **Data bias resulting from the exclusion of people who do not have access to the technologies** necessary for contact tracing to work (mobile phone, internet, etc.). For instance, the most vulnerable are least likely to own a smart device and only about 50 per cent of the world population has access to the internet (essential for the technologies to work).[11]
- **Without mass testing campaigns** to determine who is infected, digital tools will not help as the technologies used for contact tracing aim to **determine proximity to those carriers who have been diagnosed**. If a significant proportion of the population is untested and cases go undetected, contact tracing is unlikely to contain the spread of the virus.

Finally, it should also be noted that, at this time, a robust, publicly available body of research on the efficacy of the various approaches to digital contact tracing within different public health responses and contexts is simply not available.[12]

Location tracing

This type of tracing determines the location of people and is primarily used for surveillance. Positive uses of location tracing allow for the determination of hot spots for infection, and the impacts of local ordinances to reduce congregations of people. It may also be used to monitor compliance with quarantine orders through active tracing of known cases.

Collecting and storing the data

Mapping GPS data: For most location tracing based on GPS technology or device location, the data are captured and stored centrally. Some mobile network operators and smartphone-focused companies work with government to analyse where people are congregating, to get a real-time sense of social distancing measures or reductions in general movements or to understand aggregate travel patterns for epidemic modelling. Understanding general population movements, infection hot spots and compliance with local ordinances does not require individual users to be identified. But individual identification might be possible if aggregations include a low number of individuals and insufficient care has been put into the aggregation techniques. In some cases, data can be used in an anonymized manner, but even if the best contemporary approaches are used, they may remain susceptible to de-anonymization techniques.[13] More privacy-conscious use of the different modalities of mobile phone data sharing have been advocated by organizations such as the European Data Protection Board.[14]

[11] International Telecommunication Union, *Measuring the Information Society Report 2018*, ITU, Geneva, 2018.

[12] Ada Lovelace Institute, *Exit through the App Store? A rapid evidence review on the technical considerations and societal implications of using technology to transition from the COVID-19 crisis*, Ada Lovelace Institute, London, 20 April 2020. Available at: <www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf>, accessed 25 May 2020.

[13] de Montjoye, Yves-Alexandre, et al., 'Unique in the Crowd: The privacy bounds of human mobility', *Scientific Reports*, vol. 3, no. 1376, 2013. Available at: <www.nature.com/articles/srep01376.pdf>, accessed 25 May 2020.

[14] de Montjoye, Yves-Alexandre, et al., 'On the Privacy-conscientious Use of Mobile Phone Data', *Scientific Data*, vol. 5, 2018, available at: <www.nature.com/articles/sdata2018286/?source=techstories.org>, accessed 25 May 2020; *Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak.*

Using big data: Other approaches include analysing big data – for example, by mining social media posts and/or spending data using computational techniques such as machine learning or artificial intelligence – to identify infection hot spots or predict virus spread at the aggregate data level. The Canadian company BlueDot used mined data from social media accounts to predict the initial spread of COVID-19 from China to Thailand, providing one example of the use of big data for surveillance.

Limitations of the use of GPS data and big data for surveillance

The number of limitations in relation to the use of GPS data and big data include that:

- only people with a mobile phone will be represented in the data and, consequently, children will frequently be under-represented in the data
- only people with GPS-enabled smartphones will produce accurate locations
- people who use the technology more often may be over-represented in aggregate data.

Therefore, using these data without careful attention to these biases is likely to produce insights that overlook the needs and situation of poor communities that lack access to mobile phones.

Using biometric technologies: Facial recognition has also been used for location tracing for surveillance, notably in countries such as China, Israel, the Republic of Korea, the Russian Federation and Singapore. Where used, this approach is generally managed through government infrastructure and involves running facial recognition software (or algorithms) either over live camera feeds or still images (e.g., captured by closed circuit television or drones) to match persons of interest – such as confirmed cases – against biometric templates stored in a central database. This ‘active’ surveillance requires that persons of interest are embedded in a biometric database, either through a specific image capture of their face or by linking health records (such as a positive test result) to another government identification system. The technology is also used to identify individuals who are breaking control measures, such as social distancing in public spaces, by matching their image to those stored in a population database.

Facial recognition is also being used in a quite different manner for active monitoring of known cases or ‘at risk’ individuals, who are subject to a strict quarantine order. Individuals are asked to download a specific application and to log in each day to take a ‘selfie’ using their mobile phone camera. This photograph is then matched against the biometric template used to enrol the individual when the application was set up (or drawing on a recognized government identification system). It is then possible to confirm that the phone is in the possession of the person under the quarantine order, and data are matched to the location data of the device to confirm the individual’s compliance with the order. Unlike broader public surveillance, which matches an image on camera to a database of individuals to seek a potential match (and which therefore must be managed as a centralized system), this approach uses one-to-one matching, so decentralized data can be stored on individual devices once set up to do so. Similar approaches to confirming identity are also starting to emerge in relation to university exams and online classes. New approaches to online platforms are being rolled out in response to the current crisis, and are a common feature of private sector platforms used to secure payments.

Limitations to the use of biometrics

Aside from concerns regarding future identification via data linkages, and who has access to use tracking data on individuals, facial recognition has a number of potential limitations and biases, including:

- less reliable matching for children's faces[15]
- potential biases or differences in matching accuracy for people with darker skin, depending on the sensors and algorithm used[16]
- difficulties rectifying incorrect results, such as a false positive, given the permanence of data linked to a biometric trait[17]
- importantly, its costly infrastructure is not easily dismantled post-COVID-19 (unlike uninstalling an application) and can be easily repurposed for aims unrelated to public health.

Key points. Getting to the heart of the issue: How digital data are collected and stored for contact tracing and surveillance

There are two primary forms of tracing:

- **Digital proximity tracing**: Digital proximity tracing involves determining proximity between devices or to the location history of an infected individual, and is used to determine whether an individual has come into contact with potential carriers of COVID-19. These data are primarily used for contact tracing.
- **Location tracing**: Location tracing is primarily about providing surveillance to determine locations of people to ascertain the efficacy of social distancing measures and 'lockdown' orders.

- **Digital proximity tracing** can be undertaken using technologies that do not require any central collection of data (e.g., Bluetooth technology) and/or can be achieved through the collection of de-identified data without violating individual privacy. There is currently no robust evidence on the efficacy of the use of proximity tracing to contain the COVID-19 pandemic within various regulatory frameworks and contexts.
- Unless a government has in place mechanisms that allow people to self-isolate (and people are prepared to do so) and also has the resources and systems to allow for testing on a significant scale, contact tracing will be of doubtful benefit.

[15] Deb, Debayan, Neeta Nain and Anil K. Jain, 'Longitudinal Study of Child Face Recognition', in *2018 International Conference on Biometrics*, 2018, pp. 225–232, available at: <https://ieeexplore.ieee.org/document/8411226>, accessed 25 May 2020; Best-Rowden, Lacey, Yovahn Hoole and Anil Jain, 'Automatic Face Recognition of Newborns, Infants, and Toddlers: A longitudinal evaluation', in *2016 International Conference of the Biometrics Special Interest Group*, 2016, available at: <https://ieeexplore.ieee.org/document/7736912>, accessed 25 May 2020.

[16] Corby, Patricia M., et al., 'Using Biometrics for Participant Identification in a Research Study: A case report', *Journal of the American Medical Informatics Association*, vol. 13, no. 2, March–April 2006, pp. 233–235, available at: <www.ncbi.nlm.nih.gov/pmc/articles/PMC1447546>, accessed 25 May 2020; Buolamwini, Joy, and Timnit Gebru, 'Gender Shades: Intersectional accuracy disparities in commercial gender classification', *Proceedings of Machine Learning Research*, vol. 81, 2018, pp. 77–91.

[17] False positive: The presumption of infection when the person is not infected.

- **Location tracing** allows for aggregate data to be used to determine where people are not adhering to social distancing measures, without requiring individuals to be identified.
- **Facial recognition for surveillance** poses a number of privacy concerns as it is less robust in identifying children, may be difficult to contest, and may be difficult to dismantle and easy to repurpose. Further, **use of GPS data and big data is subject to bias** in relation to who is captured and how frequently.

THE VALUE AND RISKS OF THE USE OF DIGITAL TECHNOLOGIES FOR CONTACT TRACING AND PUBLIC HEALTH SURVEILLANCE

The value

The Director-General of the World Health Organization has referred to contact tracing as part of the "backbone of the response" to COVID-19, noting that one "cannot fight a fire blindfolded[18]." Digital technologies enhance national and local capacities to reach greater numbers of people, reduce costs relative to manual contact tracing, and allow for quicker and easier collection and analysis of relevant data. Further, they are not dependent on individual recall of proximity, which simply may not be possible in relation to strangers. They may also help to minimize the need for large call centres or face-to-face interactions by public health officials that may put their own staff at risk.[19]

Some less invasive digital approaches, such as those involving decentralized applications, allow for people to self-identify as being 'at risk'.[20] Invested with sufficient public support and trust, such an approach would allow individuals who believe they may have the virus to anonymously identify potential contacts and choose to self-isolate. The value of this approach lies not only in the reduced pressure where testing kits are scarce, but also in the retention of privacy and control of personal data and the avoidance of potential stigma attached to a diagnosis.

While it appears that children may be less susceptible to COVID-19 than adults, many with underlying conditions or other vulnerabilities may still be affected. Further, children and young people are also likely to be among those most significantly impacted by the secondary socio-economic impacts from the pandemic, many of which may have lasting impacts on their life course. It is therefore imperative that we ensure the responsible use of data available to support the response to, and mitigation of, the pandemic. Using digital technologies for contact tracing and surveillance has significant potential to help governments and partners substantially improve their knowledge of how the virus is spreading in and affecting communities and, subsequently, to implement more effective containment measures faster to mitigate those impacts.

[18] Adhanom Ghebreyesus, T., *WHO Director-General's opening remarks at the media briefing on COVID-19 – 16*, March 2020, available at, < https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---16-march-2020>

[19] Ada Lovelace Institute, Exit through the App Store? A rapid evidence review on the technical considerations and societal implications of using technology to transition from the COVID-19 crisis, Ada Lovelace Institute, London, 20 April 2020. Available at: www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf>, accessed 25 May 2020.

[20] Decentralized in this context refers to data that mostly remain with the primary owner rather than being collected and processed centrally.

Risks

Despite the obvious benefits of these digital technologies, their current designs, attendant policies and applications have raised a number of concerns among civil society, journalists and academia. Though many of these concerns apply to the broader population, they are still relevant to and likely to affect children and their families and communities. Concerns include systemic risks, impacts on individuals and communities, and child-specific risks.

Systemic risks

- The speed of the roll-out of the technologies and the bypassing of traditional checks and balances, resulting in a lack of scrutiny and oversight from the communities affected by them.
- In a significant number of contexts, clearly identified measures to reduce surveillance and data collection (including by third parties) when the COVID-19 crisis is over are lacking, resulting in risks to the future restoration of rights.
- The use of expensive technologies such as smartphones, potentially further marginalizing already disadvantaged groups in society and exposing them to greater risks.
- The undermining of important manual contact-tracing systems that are well established and accessible to all, not just those with access to technologies such as mobile phones.
- Where there has been investment in physical and technological surveillance infrastructure and systems, dismantling these technologies will be difficult and they may be easily repurposed for aims unrelated to public health. This is notably true for facial recognition hardware and systems.
- Digital contact tracing has greater efficacy with more wholesale coverage.[21] Further, in many instances it is contingent on self-reporting. Without trust in public institutions, uptake of a contact-tracing application is likely to be low and thereby its efficacy will be reduced. Further, if use of such an application is mandated by law without consultation or explanation and clear governance mechanisms, this may erode public trust.
- Contact tracing without testing could potentially lead to unnecessary quarantining of individuals and, consequently, to unnecessary restrictions of rights.

Impacts on individuals and communities

- Potential loss of privacy, and data sharing in the public arena or to a much broader set of 'authorized' users (in some instances, providing this information publicly, in real time). Data sharing may involve data that individuals have knowingly supplied to a data collection process or data that they are unaware have been used in this manner or which have been accessed without their knowledge. Privacy violations, which may arise when personally identifiable data are shared without the consent of the data subject, raise the spectre of potential re-identification through the future merging of databases.
- Potential longer-term losses in personal privacy where clear measures to reduce surveillance, and transparency in measures to restore privacy rights are not in place.

[21] Hinch, Robert, et al., Effective Configurations of a Digital Contact Tracing App: A report to NHSX, University of Oxford, Oxford, 2020.

- Stigma and discrimination resulting from the public identification of an individual as infected or as residing in an area identified as high risk.
- Coercion/pressure to share data (lack of true consent/willingness) including 'voluntary' uptake of applications.
- Risk of misidentification of individuals through inaccurate facial recognition, leading to accusations of the breaking of lockdown rules, with limited recourse for individuals to contest the accuracy of the identification.
- Similarly, risk of inaccurate determination, via Bluetooth and GPS technologies, of exposure to the virus (false positive), negatively affecting an individual's anxiety levels and potentially unnecessarily restricting her/his freedom of movement.
- Risk of false negatives and the potential for critical cases to be overlooked where testing is entirely or largely replaced by, and dependent on digital contact tracing.[22]
- Increased concerns regarding data protection and the risk of personal data being 'hacked' or available to unauthorized users as more data are collected, linked, transmitted and shared with a broader range of users and as new systems are introduced at speed.
- Risk of certain communities becoming invisible to a health system that relies blindly on data sets gathered from technologies that communities do not possess, effectively excluding them from data sets used to inform health services and policies .[23]

Child-specific risks

While many of the same issues and concerns may affect children, the impacts of these risks on children may be quite different to their impacts on the adults in the children's lives. The RD4C principles recognize that the concerns relating to the use and protection of children's data are unique and therefore deserve special attention. This need for additional and explicit consideration of and reflection on the impacts on children stems from the following risks:

- The technologies are frequently not designed to consider children and may, in fact, perform poorly when applied to children (e.g., facial recognition).
- Children are likely to have less agency over their own data and parents and caregivers may not understand the impacts on their children's privacy. As children may also be less able to identify avenues for and seek redress of errors or data breaches, they may be disproportionately affected by such incidents if and when they occur.
- The employment of 'nudge' techniques in the design of these technologies may encourage children to provide more personal data than they would otherwise volunteer.[24]

[22] False negative: The presumption that a person is free from infection when in fact the individual is infected.

[23] Crawford, Kate, 'The Hidden Biases in Big Data', *Harvard Business Review*, 1 April, 2013, <https://hbr.org/2013/04/the-hidden-biases-in-big-data>, accessed 25 May 2020.

[24] 'Nudge' techniques are approaches that take into account psychological, physical and social factors to encourage specific choices and behaviours.

- A parent or caregiver may upload or install applications or systems on a child's mobile phone in accordance with or against the wishes of the child.[25]
- Children may be more susceptible to the risks of stigma and discrimination if identified as infected. They also face longer-term implications for the development of their personal identity and with regard to potential future opportunities where public shaming occurs.
- Children may face specific safety risks if their location is known or their contacts or details are made public (or can be accessed by a broader group of users).
- Children are more susceptible to any longer-term retention of data, resulting in the greater possibility of future data linkages and identification. Further, they are likely to suffer the longest if data collection and limitations on certain privacy rights become permanent.
- Data collected from children may negatively affect their educational, employment, financial or social opportunities later in life.

With respect to the use of children's digital data for contact tracing and surveillance, there are a number of issues that differentiate children from adults and lead to child-centric concerns:

- In a number of countries, it is illegal to collect children's personal, identifiable data online. More broadly, a greater burden is placed on society to protect children and their rights (including the right to privacy) under international human rights law and other legal frameworks for the protection of children.
- Children are much more likely to be effective carriers of COVID-19 than they are to fall ill from the virus. Hence children are less likely to be singled out in debates and concerns related to COVID-19. This difference in presentation of the disease implies that contact tracing among children may need to be fundamentally different than for adults.

Hence while children are less likely to be singled out in debates related to COVID-19, serious concerns remain in relation to tracking of children, use of children's data and potential impacts of public identification of a child as a COVID-19 carrier.

[25] The Coronavirus (Safeguards) Bill 2020, United Kingdom of Great Britain and Northern Ireland, has argued that children over 13 years of age should have the right to veto the installation of or delete an application. See: <https://osf.io/preprints/lawarxiv/yc6xu>, accessed 25 May 2020.

Key points. The value and risks of the use of digital technologies for contact tracing and public health surveillance

- Large-scale testing campaigns are central to the COVID-19 response, but contact tracing and public health surveillance may be useful complementary tools. The more we know about the outbreak, the better we can contain the virus and mitigate its impacts. There is huge demand from communities for information on how to keep themselves safe and digital technologies offer the potential to provide this information.

- Digital contact tracing and surveillance enable better reach, coverage and speed of detection and, in some instances, greater accuracy (compared with personal recall). They also allow for direct communication with those 'at risk'.

- But there are also a number of systemic issues and risks related to technology use and data collection for contact tracing and surveillance, including the:

  - need for access to smartphones and internet connectivity for many contact-tracing applications, with the consequent marginalization of those disadvantaged communities unable to afford such technology
  - speed of the roll-out of the technologies and the bypassing of traditional checks and balances, resulting in a lack of scrutiny and oversight from the communities affected by them
  - difficulty of removing restrictions on rights and privacy when the COVID-19 crisis is over without clear and comprehensive planning.

- There are also risks to and impacts on individuals and communities, including:

  - stigma and discrimination that could result from the public identification of an individual as infected or as residing in an area identified as high risk
  - loss of privacy and basic rights, with no clear indications of when, how or if these infringements rights will be restored
  - coercion to participate in contact tracing, and negative impacts of false positives on exposure, risk, and perceptions of violations of ordinances.

- Children require explicit consideration when technology is used and data are collected. But they are frequently overlooked in discussions about the impacts and accuracy of the technologies adopted and the data collected. This is why UNICEF initiated the RD4C project in partnership with GovLab.

- Children are likely to be more psychologically vulnerable to any public dissemination of information about their status and movements. They are also likely to experience greater longer-term impacts of reduced privacy rights and other negative by-products of surveillance.

- Children are much more likely to be effective carriers of COVID-19 than they are to fall ill from the virus. Hence children are less likely to be singled out in debates and concerns related to COVID-19. This difference in presentation of the disease implies that contact tracing among children may need to be fundamentally different than for adults.

- Serious concerns still exist , in relation to the tracking of children, use of children's data and potential impacts of the public identification of a child as a COVID-19 carrier.

KEY MESSAGES

Upholding children's rights – and indeed those of their families – in regard to contact tracing and surveillance requires a careful balancing of risks. The risks of adopting a proposed technological solution must be weighed against the risks of not having the data it would provide to inform public health responses. Careful attention should be paid to exploring and identifying the widest possible range of potential strategies for mitigation of concerns, and to consider the appropriateness of any technological solution or approach against tests of legitimacy, necessity and proportionality.

It should be noted that not all of the risks outlined in this working paper can be adequately controlled for and, consequently, decision-making is not only difficult but also highly context-specific. What is an acceptable risk and mitigation strategy in one setting may be highly inappropriate in another. The rate of disease transmission, availability of services for those identified as infected, transparency of and trust in the authorities, public sentiment, and extent of the infrastructure and existing governance around data rights and protections will all affect these decisions. Given this complexity, the principles outlined by the RD4C project provide a useful framing to put the best interests of the child at the centre of our work and to shape key advocacy messages for governments, development partners and industry alike.

The following are the key messages in relation to general and child-specific ethical issues in the use of digital technologies for contact tracing and surveillance. This section outlines in detail, and in accordance with the RD4C principles, recommendations to ensure that human rights are explicitly considered in the adoption, implementation and decommissioning of digital tools and to ensure that use of such tools, or the approach adopted, is consistent with clear public health goals and outcomes.

Purpose-driven

Data collection should be undertaken with a clearly articulated purpose, which is both consistent with programming to support children and families and must be directly relevant to the decisions that need to be made within that context. This principle should also prevent 'scope creep' – that is, secondary uses of the data that go beyond the initial purpose of (and consent for) the data collection.

Purpose-driven

Key message 1: Data collection and use associated with any new or modified use of digital technologies for contact tracing or surveillance should be limited by the centrally defined purpose of thetechnology applied n. This means that:

- the purpose must be clearly defined, directly address a clear public health goal and be publicly documented
- data collection must be limited to what is directly required to achieve the central purpose of the system
- data should not be repurposed for other uses.

Proportional

Digital contact tracing or legitimate public health surveillance does not necessarily require identifiable data and can be carried out by many applications without centralized data collection and processing. For example, the centralized collection of individual GPS tracking data with their identifying information is unnecessary for contact tracing, as is the use of facial recognition software. Decentralized approaches are being developed –that can allow individuals to self-monitor, retain control of their data and ensure their personal safety (and that of other household members) without fear of stigma.

Proportional

Key message 2: Aggregate data should be used in preference to anonymized data wherever possible. Further, de-identified or anonymized data should be used in preference to identifiable data wherever possible and blanket population surveillance options (such as active facial recognition in public spaces) should be discouraged. Alternative approaches that may be more appropriate include use of:

- de-identified data to be stored on a central server with secure encryption keys
- peer-to-peer data exchange via Bluetooth technology, with all or most personal data residing only on the user’s device
- GPS data to be stored and retained on the user’s device (if necessary, only encrypted, aggregate data that are stored centrally should otherwise be used).

Professionally accountable

Professional accountability is essential at all levels of a digital contact tracing or surveillance programme. This includes accountability for the impacts (both positive and negative) of legitimate use of the technology on the individuals and communities among which it is deployed, as well as accountabilities for preventing or remedying inappropriate use by those with access to the system. At the health system level, it is not enough for a new data collection process such as digital contact tracing or surveillance to be purpose-driven; there must also be accountability and transparency in relation to the capacity to use the data findings to effect changes to programming.

Due diligence is essential and requires appropriate understanding and design of the technological solution to ensure accuracy of the technology for different population groups and explicitly taking into account gaps in knowledge around untested or new technologies. In a number of instances, including where biometric technologies are used, testing can and should be done wherever possible prior to or in the initial phases of implementation to determine false positive or false negative rates – and, consequently, whether a technology should be modified accordingly or rejected.[26] Clear reflection is also required on the potential for, and the impact of – on individuals and on health systems – false positive and false negative results acquired through contract tracing or surveillance.

[26] In some instances, where the data collected are de-identified, testing can be done via volunteers.

Finally, in the broadest sense, there must also be accountability to affected populations in so far as increased control and oversight during the COVID-19 pandemic should not result in a corresponding erosion of democracy and accountability, either in terms of the implementation of measures or their removal.

Professionally accountable

Key message 3:
Contact tracing and surveillance data collection should only be undertaken where:

- There is capacity to use this information to inform individuals and families at heightened risk of COVID-19 infection of the appropriate actions to take
- Where mass testing is possible. This is necessary not only to alleviate concerns raised by notification of potential exposure and the need to self-isolate, but also to ensure that the technology can, in fact, adequately prevent the spread of the disease – something that is dependent on diagnosis
- Where it can be evidenced that the technology is sufficiently accurate to meet its intended purpose
- Where it is used to inform planning, containment, response or monitoring.

Key message 4: Governance structures must include obligations of partner organizations and companies, including the requirement to restrict third party data transfers in the absence of informed consent, and/or a clear legal mandate that is consistent with the original purpose of the data collection.

People-centric

According to the RD4C principles, data and data systems that are ‘people-centric’ are those that ensure that “the needs and expectations of children, their caregivers, and their communities are prioritized by actors handling data for and about them.”[27] In the context of the COVID-19 pandemic, this means that decisions about whether to undertake digital contact tracing or surveillance, and about which technologies and systems to use to support such approaches, should be driven by local context and needs. Such decisions should not be based on political, industry or commercial interests or relationships.

‘People-centric’ approaches also require explicitly accounting for how the technology may affect different population groups (including children, women, people with disabilities, displaced people and other vulnerable groups within the subject population) in different ways, both in the design and implementation of the technology and in the analysis of findings. Differences may arise due to factors such as the accuracy and performance of digital technologies in relation to specific groups, the

[27] United Nations Children’s Fund and GovLab, Responsible Data for Children, <https://rd4c.org>, accessed 25 May 2020.

different environments in which groups live or the different resources (including technologies) that groups are able to access.

People-centric

Key message 5: The design, adoption and use of any digital platform/technology for contact tracing or surveillance should be driven by the best interests of the community, informed by an explicit understanding of how specific population groups – including children, women and other potentially vulnerable groups – may be differentially impacted by the technology.

Participatory

Although the need for rapid action in response to the changing pandemic conditions may limit broad engagement with children and communities in the design and roll-out of contact tracing and surveillance technologies, the cultural and social acceptability and appropriateness of any technological solutions is essential.

Consultation with and engagement of the community should be encouraged as early as possible in the process and preferably throughout the process including formal reviews of lessons learned at various stages – with inputs from children and other community members. At a minimum, people-centric design (as outlined above) should be adopted, with a strong focus on building trust with the community, through support for community organizations and/or individuals, to highlight – and engage with data authorities about – critical concerns or incidents as they arise.

Participatory

Key message 6: Community engagement should occur as early as possible in the design, implementation and review of contact-tracing and surveillance technologies.

Key message 7: A strong, transparent framework of system governance that seeks to foster and maintain trust within the community is critical. It must include clearly accessible mechanisms that individuals and communities can use to identify and report concerns and incidents as they arise, and to receive feedback on the subsequent responses.

Protective of children's rights

Data risks for children require specific attention. While children are likely to be affected by many of the same issues as adults, how these risks affect children's lives is likely to be substantially different, with potentially longer-term impacts. When adopting an approach that explicitly takes into account children's rights, attention must be paid to critical issues pertaining to data access and privacy, with due consideration of international human rights law and other legal frameworks for the protection of children and their privacy.

Moreover, children of different age groups may face different risks and vulnerabilities. Children's ability to grasp the situation will also differ to a large extent according to age. Thus, the information provided to children as to the purpose of data collection and use of their data should be sufficiently clear and accessible to each age group targeted by the technology.

Further, in any approach that considers children's rights, recognition is required of the potential for discrimination or shaming of individuals or communities as a result of the public dissemination of contact-tracing outcomes or surveillance findings. Within any child-centred approach, avoiding the public identification of individuals – especially children – is critical.

The Sustainable Development Goals also highlight the importance of leaving no child behind. People in impoverished communities and circumstances may not have access to relevant technologies.[28] As such, they may be unable to access critical services, such as contact-tracing notifications, or may not be represented in critical data obtained from mobile phones or other devices. This is despite the fact that these vulnerable groups are more likely to live in circumstances where they are more vulnerable to infection (i.e., crowded, high-density places and spaces) than the rest of the population. They are also more likely to struggle to bear the economic costs of the direct and indirect impacts of COVID-19. Children in such contexts are also likely to be asymptomatic vectors, further complicating issues relating to identification, inter-dependencies and the need for mass testing in these communities.

Protective of children's rights (and those of their communities)

Key message 8: While many population-wide privacy risks apply to children, they need to be explicitly considered when reflecting on the impacts of digital contact tracing and surveillance. This is necessitated by children's predominantly asymptomatic profiles and the potential for significant longer-term personal impacts. The design and implementation of any digital contact-tracing or surveillance programme should explicitly reflect international human rights law and other legal frameworks for the protection of children and their privacy.

Key message 9: Contact-tracing or surveillance systems and technologies should adopt a 'privacy by design' approach, and technologies should maximize individual privacy and agency. For instance, the technology/approach chosen should allow for the retention of personal data and for individual redress mechanisms, such as data correction and deletion, wherever possible.

[28] An example is the Apple and Google software that is being developed which it is claimed will require Android phones and iPhones to have the latest operating system. This is unlikely to be the case for those with limited resources.

Key message 10: Wherever possible, informed consent should be factored into the design of digital contact-tracing or surveillance systems. Where this is not possible to uphold in practice, this should be explicitly acknowledged in the design, which should be supported by strong and transparent governance and accountability mechanisms.

Key message 11: Access and equity should be explicitly considered in the design and use of technologies for digital contact tracing and public health surveillance. Clear strategies for equitable public health outcomes should be in place where digital solutions are likely to disproportionately (and potentially negatively) affect marginalized communities. Individuals should not be penalized for lacking access to relevant technologies for the purposes of contact tracing or surveillance. In such instances, mixed approaches combining manual and digital contact-tracing services should be used.

Key message 12: Individuals should not be compelled to upload or install relevant applications or systems unless warranted by legitimacy, necessity and proportionality tests. In the absence of robust evidence on the efficacy of applications/systems, and in the absence of their widespread adoption, these standards are currently unlikely to be met.

Prevention of harms across the data cycle

Foreseeable harms should be identified and all possible efforts made to prevent these arising over the course of the data cycle. Prevention of harm should be considered in decisions about who is included in the data collection in the first place and about how data are managed and handled from the time of collection through to their ultimate destruction.

Public health surveillance in a pandemic is ultimately time-sensitive and time-bound. Therefore, consistent with the principle of being purpose-driven, surveillance measures would require a ‘sunset clause’ in relation to the terms and timing of the destruction of centralized data. This is particularly relevant for identifiable data but remains relevant for all data provided on the premise (and with the consent) that they are to be used specifically for contact tracing or public health surveillance. Where there is a possibility that data may be used to improve the management of future public health crises, this should be stated in advance; at a minimum, data can be de-identified and a clear and public announcement made to provide justification for their use at a later date.

Prevention of harms across the data cycle

Key message 13: Data rights and protections should be upheld to the fullest extent possible. If there is any suspension or relaxation of these as a result of the introduction of digital contact-tracing or surveillance measures, such a change must be:

a) clearly articulated, with justification given for the need for the change

b) considered in relation to the impacts on vulnerable groups and appropriate mitigation strategies put in place

c) time-bound, with the full provisions restored as soon as possible.

Key message 14: Prior to any centralized collection of data for the explicit purpose of contact tracing or public health surveillance, or as soon as reasonably practicable, clear terms should be established within relevant regulations in regard to the duration of storage and timing of the destruction of the data. Such terms should be in place for manual systems and should be reviewed and adapted for any new digital/technology-based system.

FURTHER INFORMATION

To find out more about the Responsible Data for Children project, visit: <www.rd4c.org>
UNICEF guidance on the use of biometric technologies is available at: <https://data.unicef.org/resources/biometrics>

Download the UNICEF resource *Children's Online Privacy and Freedom of Expression: Industry Toolkit* at: <www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf>

View the UNICEF discussion paper 'Ethical Considerations for Evidence Generation Involving Children on the COVID-19 Pandemic' at: <www.unicef-irc.org/publications/1086-ethical-considerations-for-evidence-generation-involving-children-on-the-covid-19.html>

To find out about the UNICEF Manifesto for Good Governance of Children's Data, see: <www.unicef.org/globalinsight/data-governance-children>

APPENDIX A. COMPARISON OF PROPOSED INTERNATIONAL DIGITAL CONTACT-TRACING APPLICATIONS

App	Mandatory or voluntary	Protocol	Data collected	Data access	Infection reporting	Contact alerting	Actions
NHS app (in development)	Voluntary	To be determined	IDs created by nearby phones	User and public health authorities	Self-reported and by medical professionals	To user and medical professionals	Quarantine if infection reported by medical health professionals
Singapore Trace Together (live)	Voluntary	Bluetrace	IDs created by nearby phones	User only	Medical professionals	To user and medical professionals	Decided by medical professional
South Korea (live)	Mandatory	Not applicable	Citizen location information, credit card data	User and public health authorities	Self-reported and by medical professionals	To user and medical professionals	Quarantine
Taiwan (in development)	Mandatory	Not applicable	Citizen location information, credit card data	User and public health authorities	Self-reported and by medical professionals	To user and medical professionals	Quarantine
Germany, France, Estonia and other EU countries (in development)	Voluntary	PEPP-PT	IDs created by nearby phones	To be determined	To be determined	To be determined	To be determined
Israel (live)	Mandatory	Not applicable	Citizen location information, credit card data	User and public health authorities	Self-reported and by medical professionals	To user and medical professionals	Quarantine

Source: Ada Lovelace Institute, *Exit through the App Store? A rapid evidence review on the technical considerations and societal implications of using technology to transition from the COVID-19 crisis*, Ada Lovelace Institute, London, 20 April 2020. Available at: <www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf>, accessed 25 May 2020.

unicef

Office of Research – Innocenti