Innocenti Research Brief

2020-11

unicef
Office of Research – Innocenti

Covid-19 & Children

Digital contact tracing and surveillance during COVID-19

General and Child-specific Ethical Issues

Karen Carter[i], Gabrielle Berman[ii], Manuel García-Herranz[iii], Vedran Sekara[iv]

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

ACKNOWLEDGEMENTS

This paper summarizes the findings of the of UNICEF Innocenti Working Paper 2020-01 that 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).

INTRODUCTION

The response to COVID-19 has seen an unprecedented rapid scaling up of technologies to support digital contact tracing and surveillance. Accessible, high-quality data, based on a foundation of widespread testing, are essential to support decision-makers in government and 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. There is also huge demand from communities for information on how to keep themselves safe and digital technologies offer the potential to provide this information.

Digital technologies to enhance contact tracing and public health surveillance may be useful complementary tools in this context. The more we know about the outbreak, the better we can contain the outbreak and mitigate its impacts.

The collation and use of personally identifiable data may also pose significant risks to children's rights, however. Harm may include:

- misuse of data (by both authorized users and those accessing the data illegally)
- infringement of rights in the collection and use of data (discrimination, stigma, restrictions, and loss of privacy)
- risks to children from changes in the nature of surveillance and the accumulation of data over time – with unknown and potentially long-term repercussions.

Although the digital risks in the current environment are not wholly new, they are unprecedented in terms of speed, scale and invasiveness. There are more and varied players making decisions about how data, including children's data, are used and how related risks are assessed and handled. This means that we need to engage with a broader set of government and industry partners to ensure that children's rights are not overlooked.

Children are subject to many of the same risks as adults when it comes to digital technologies, children also require specific consideration. This is because they are:

- frequently overlooked in discussions about accuracy and impacts of the technologies adopted and the data collected
- likely to be more vulnerable to any public dissemination of information about their status and movements
- likely to experience greater longer-term impacts caused by reductions in privacy rights and other negative by-products of surveillance

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

- much more likely to be effective carriers of COVID-19 than they are to fall ill from the virus – hence contact tracing and subsequent protections for children may need to be different than for adults.

UNICEF work such as the Industry Toolkit on Children's Online Privacy and Freedom of Expression and the partnership with the GovLab on Responsible Data for Children – which promotes good practice principles and has developed practical tools to assist field offices, partners and governments to make responsible data management decisions – provides an important foundation to understand and balance the potential benefits and risks to children of data collection.

THE TECHNOLOGY

The technologies in use to better understand the nature of the COVID-19 pandemic include mobile phone tracking, biometric technologies and data scraping. These are being used to carry out two main forms of tracing: digital proximity tracing and location tracing.

Digital proximity tracing: Digital proximity tracing involves determining proximity between devices (usually mobile phones) or to the location history of an infected individual. It 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. Proximity tracing involves the use of Bluetooth technology to track signals from the devices of other users in the proximity of the individual.

Digital proximity tracing for current cases can be undertaken without any central collection of data and/or can be achieved through the collection of de-identified data without violating individual privacy. There is, however, 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.

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. Location tracing allows for the use of aggregate data, such Global Positioning System (GPS) location data from a mobile phone network, or analysis of social media posts to identify where people are congregating in real time. Alternatively, it may involve the identification of individuals, for example, through identifiable data from a mobile phone location or using biometric facial recognition. Most location tracing requires centralized storage of and access to data. Aggregate data can, however, be used to determine where people are not adhering to social distancing without requiring individuals to be identified.

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).

Facial recognition may be used to:

- match an unknown individual (such as someone breaking movement restrictions) against a population database to identify her/him (one-to-many matching)
- monitor movement in public of a known set of individuals (such as positive cases subject to a quarantine order) by matching unknown individuals to a 'watchlist' (one-to-few matching)
- require individuals subject to a quarantine order to download a specific application and upload a 'selfie' each day, used to verify identity, which is matched against the device's location data to ensure compliance with the order (one-to-one facial matching with a stored record that does not necessarily require centralized storage).

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. Bias is also an issue in the use of GPS data and big data in relation to who is captured and how frequently.

KEY MESSAGES

The following key messages, detailed in full in the working paper, are aligned with the Responsible Data for Children principles and highlight recommendations to ensure that children's rights are explicitly considered in the adoption, implementation and decommissioning of such digital tools and mechanisms.

Purpose-driven

1: **Data collection and use should be limited to achieving explicit public health outcomes**.

Proportional

2: **Only the level of identification necessary to achieve the intended public health outcomes should be used** in technologies. As such, aggregate data should be used in preference to anonymized data wherever possible, and de-identified or anonymized data used in preference to identifiable data.

Professionally accountable

3: Digital contact tracing and surveillance are only useful if undertaken in the context of (a) the **availability of widespread and reliable testing**; and (b) **sufficient resources and support** that allow for appropriate care and the capacity to self-isolate.

4: **Governance structures must include obligations of partner organizations and companies**, including the requirement to restrict third party data transfer 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

5: The use of digital technology for **contact tracing and surveillance should be driven by the best interests of the community**, informed by an explicit understanding of how specific population groups (including children) may be affected differently by the technology.

Participatory

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

7: **A strong, transparent framework of system governance** that seeks to foster and maintain trust within the community and which includes feedback and response provisions is critical.

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

8: **Children need to be explicitly considered** when reflecting on the impacts of digital contact tracing and surveillance.

9: **Contact-tracing or surveillance systems and technologies should adopt a 'privacy by design' approach**, and technologies should maximize individual privacy and agency. Personally identifiable data should only be disclosed to specific individuals who have a justified need for that information, within a clear regulatory or governance framework.

10: Wherever possible, **informed consent should be factored into the design** of digital contact-tracing or surveillance systems.

11: **Access and equity should be explicitly considered in the design** and use of technologies for digital contact tracing and public health surveillance.

12: **Individuals should not be compelled to use applications or systems** unless warranted by legitimacy, necessity and proportionality tests.

Prevention of harms across the data cycle

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.

14: **Clear terms should be established within relevant regulations in regard to the duration of storage and timing of the destruction of the data**, irrespective of who holds the data.

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>

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 directions, 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. The views expressed are those of the authors and/or editors. For rights of reproduction or translation, apply to UNICEF Office of Research – Innocenti. Short extracts may be reproduced unaltered without authorization on condition that the source is indicated. © UNICEF Office of Research

UNICEF OFFICE OF RESEARCH – INNOCENTI
Florence, Italy

www.unicef-irc.org

+39 055 20330

florence@unicef.org
@UNICEFInnocenti
facebook.com/UnicefInnocenti

For every child, answers