Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing

Interim guidance
28 May 2020

World Health Organization

Background

This interim guidance is intended to inform public health programmes and governments that are considering whether to develop or implement digital proximity tracking technologies for COVID-19 contact tracing. The document covers ethical principles, technical considerations and requirements that are consistent with these principles; and how to achieve equitable and appropriate use of such technologies.

Contact tracing is the process of identifying, assessing, and managing people who have been exposed to a disease to prevent onward transmission. When systematically applied, contact tracing will break the chains of transmission of an infectious disease and is thus an essential public health tool for controlling infectious disease outbreaks. For contact tracing to be effective, countries need adequate capacity, including human resources, to test suspect cases in a timely manner.[1] Digital technology can play a role in contact tracing programmes implemented in Member States.

Member States are obliged under the International Health Regulations to develop public health surveillance systems[2] that capture critical data for their COVID-19 response, while ensuring that such systems are transparent, responsive to the concerns of communities, and do not impose unnecessary burdens, for example infringements on privacy.[3] Failure to implement effective surveillance systems can hamper an effective public health and clinical response.[4] Digital technologies are used in public health surveillance to support rapid reporting, data management and analysis. Especially when combined with machine learning and artificial intelligence, they could constitute powerful tools that provide public health agencies with valuable information to make appropriate decisions.[5]

One form of digital technology for surveillance that has been receiving attention in many countries facing COVID-19 epidemics in recent months is proximity tracking. Proximity tracking measures signal strength to determine whether two devices [e.g. smartphones] were close enough together for their users to spread the virus from an infected individual to an uninfected person. If one user is infected, others who have been identified as within proximity of the other person can be notified, and thereby take appropriate steps to reduce health risks to themselves and others.[6] Proximity tracking is often conflated with ‘contact tracing’, although contact tracing is a broad public health discipline, and proximity tracking is a new technique for aiding contact tracing.

Digital proximity tracking, however, has its limitations. This technology cannot capture all the situations in which a user may acquire COVID-19, and it cannot replace traditional person-to-person public health contact tracing, testing or outreach which is usually done over the phone or face to face. Digital proximity tracking applications can only be effective in terms of providing data to help with the COVID-19 response when they are fully integrated into an existing public health system and national pandemic response. Such a system would need to include health services personnel, testing services and the manual contact tracing infrastructure.[7]

Considering these limitations, health authorities could use digital proximity tracking tools for notifying a person of an increased risk of exposure to another who has tested positive for COVID-19. Such notification of a person who may have had close contact with a COVID-19-positive individual could encourage the former person to seek out testing (if available) or take precautions to limit potential transmission such as self-isolation and physical distancing, even before the onset of any symptoms.[8] Early public health response actions can make a significant difference between control and a resurgence of COVID-19. Furthermore, data generated by digital proximity tracking technologies could be useful for researchers to prepare for future COVID-19 outbreaks and to assist general preparedness for future epidemics and pandemics.

Yet such uses of data may also threaten fundamental human rights and liberties during and after the COVID-19 pandemic. Surveillance can quickly traverse the blurred line between disease surveillance and population surveillance. Thus, there is a need for laws, policies and oversight mechanisms to place strict limits on the use of digital proximity tracking technologies and on any research that uses the data generated by such technologies.

Through their products, services or platforms, some private companies capture as much data as governments gather. Such companies may develop or are even sharing their own digital proximity tracking applications with governments and, in some cases, are given the responsibility for collecting and analysing the data thus harvested. Moreover, there is a broader concern that private companies may permanently integrate their commercial products, services and architecture within public health infrastructures.

Member States can achieve their public health objectives while protecting fundamental rights, such as privacy, at the same time. Moreover, laws and human rights instruments provide for use of personal data that is in the public interest, while also preventing unnecessary intrusions or commercial exploitation. Integrating these and other ethical considerations into the design (programming) of a new technology can ensure that its technical specifications preserve and promote certain values, such as transparency and privacy.

The effectiveness of digital proximity tracking to assist contact tracing remains unknown

Digital proximity tracking technologies are already being deployed in several countries for their COVID-19 response. Meanwhile, governments, universities and companies in other countries are developing technologies and scaling these up at a historically unprecedented speed. As a result, digital technologies can be widely distributed after their development in a largely unregulated environment. The effectiveness of such technologies to assist contact tracing depends largely upon the underlying technology design and implementation approach but also on other factors, such as the level of uptake and the levels of confidence and trust that a population may vest in a chosen solution.

Implementation of digital proximity tracking for contact tracing purposes in countries must be subject to rigorous review. It is essential to measure the effectiveness and impact of these technologies for building public confidence in their reliability and trust in governmental or private entities that design, disseminate and manage these technologies. Assessing their effectiveness and impact can also help to determine if the trade-off of privacy is proportional to the public health impact achieved. If such technologies do not prove effective against COVID-19, then the technology should be phased out. Currently, there are no established methods for assessing the effectiveness of digital proximity tracking. More research to evaluate their effectiveness is needed and, ultimately, robust methodologies need to be developed for this purpose.

Enabling environment for use of digital proximity tracking applications

While digital proximity tracking applications could play a useful role in supporting contact tracing for COVID-19, these technologies are only one intervention within a wider system of policies, interventions, and investments. Governments and health systems should explain to the public how this mix of policies, interventions and technologies would work together within an overall strategy.

Even if a digital proximity tracking application works in one country, these technologies may only be effective in other countries with sufficient technological infrastructure and safeguards to ensure ethical use. First, a country must already have widespread diffusion of smartphones or other appropriate devices and Internet access. Recent studies have estimated that a digital proximity tracking technology should be adopted by 60% to 75% of a country's population to be maximally effective for contact identification.[9, 10]

Data protection and privacy laws need to be in place, supported by additional legislation to provide a legal basis (and limits) for data processing, restrictions on data use, measures to establish oversight, and sunset clauses to dismantle a given technology.[11] In addition, a certain level of trust in government is needed, otherwise individuals are unlikely to use digital proximity tracking applications in the first place, even if usage is entirely voluntary. Finally, communities themselves need to understand how such tools work, not least to avoid potential discrimination or unfair targeting. Inclusive communication strategies that explain the rationale for implementing these technologies and how they will be used should be designed so that they reach marginalized populations and vulnerable communities. Users need to be well informed, so that they do not develop a false sense of security when using such technologies.

Inequities could be exacerbated through the use of these technologies.[12] Digital proximity tracking applications only indirectly benefit those individuals without access to smartphones or other appropriate devices, and in general will only benefit those who are already comfortable using smartphones. Reliance on digital proximity tracking for contact tracing, to the exclusion of the traditional approaches, will reduce access to essential services for the marginalized populations, especially the elderly and people living in poverty. Where appropriate, steps should be taken to improve voluntary access to such technologies in resource-limited settings, for example through lower mobile data costs or improved affordability and accessibility of low-cost devices.

Suggested principles

To provide governments, public health institutions, non-State actors (nongovernmental organizations, charities, foundations) and companies with guidance as to the ethical and appropriate use of digital proximity tracking technologies to address COVID-19, the following principles have been identified:

Principle	Explanatory Text
Time limitation	All measures shall be temporary in nature and limited in scope. If governments and health systems expand monitoring and surveillance powers then such powers should be time bound, and only continue for as long as necessary to address the current pandemic. Measures should be fully withdrawn at the earliest moment after the epidemic has ended locally. There are legitimate concerns that digital proximity tracking will be unnecessary yet will remain in place.
Testing and evaluation	Digital proximity tracking technologies are novel and largely untested in many countries and settings. Every effort should be made to test the technologies prior to widespread use to ensure they function as intended, are technically robust, and have no security flaws. Governments and health systems should implement rigorous evaluation of the technology during the pandemic to continuously monitor that it is working effectively. The evaluations should be conducted by an independent agency or research body and should be published.
Proportionality	Collection and processing of personal data and health data shall be proportionate and provided by law. This means that collection of data for digital proximity tracking must be (a) justified by legitimate public health objectives; (b) suitable to achieve the intended goal; (c) necessary; and (d) reasonable and proportionate to the aims pursued. The latter requirement entails assessing the value of colliding rights vis-à-vis the impact intensity of surveillance activities on each person. The least intrusive (privacy-preserving) measures should always be preferred for an application's design, including avoiding the use of physical location (geographic position) tracking for digital proximity tracking.
Data minimization	Data collection, retention and processing shall be limited to the minimum necessary amount of data that is needed to achieve the public health objective. Thus, data collection should not require the identity or location data of a user, or a time stamp of a proximity event (though the date of a proximity event may be useful). Data collected, retained and aggregated must be limited in scope.
Use restriction	The sale and use of data for commercial purposes or advertising activities should be strictly prohibited. Recognizing that governments may have existing data protection laws and frameworks already in place, the sharing of data with government departments, agencies or third parties that are not involved in the public health response should be prohibited. The sharing of data with law enforcement or immigration departments or agencies should also be prohibited.
Voluntariness	An individual's decision to download and use an application that contributes to public health surveillance or digital proximity tracking should be voluntary and informed. Governments should not mandate use of such an application. Additional incentives or inducements by either a government or private parties should not be offered to individuals who download and use such an application. No individual should be denied services or benefits from either a government or private parties for refusing to use an application, including the right to use health services, the receipt of economic aid in the context of a pandemic or thereafter, or the use of a phone that is provided by a company for work-related purposes. An individual should be free to turn off the application at any time and should be free to delete the application at any time, without any consequences, as well as to delete any data that may have been collected and stored, including retroactively redacting blocks of time that the user does not wish to upload.
Transparency and explainability	Data collection and processing shall be transparent, and individuals shall be provided with concise and reader-friendly information in clear and unambiguous language regarding the purpose of collection, the types of data collected, how data will be stored and shared, and how long data shall be retained. There should be full transparency about how the applications and application programming interfaces (APIs) operate, and publication of open source and open access codes. Individuals should also be provided with meaningful information about the existence of automated decision-making and how risk predictions are made, including how the algorithmic model was developed and the data used to train the model. Furthermore, there should be information about the model's utility and insights as to the types of errors that such a model may make.

Principle	Explanatory Text
Privacy-preserving data storage	There are differing views as to whether data storage should be decentralized or centralized, including which approach to data storage is more effective and secure. Both approaches may preserve privacy but both approaches also have vulnerabilities that must be addressed, including the security of data that are collected and stored. There is an emerging consensus, including opinions issued recently by several data protection authorities, that decentralized approaches enhance privacy, since they provide users with greater control (including the exercise of consent or withdrawal of consent) over the quantum of information that a user may share with health authorities. The collection and use of such data by health authorities can therefore be limited to what is strictly necessary for the operation of a digital proximity tracking system. Whichever approach is selected, governments and third parties should ensure it is in conformity with expectations of privacy and the principles included in this guidance.
Security	Every effort should be made to ensure high security, including encryption, of any personal data or health data collected and of any devices, applications, servers, networks, or services involved in collection, transmission, processing, and storage. Applications should be subject to third-party audits and penetration testing, and developers should publish full details about their security protocols.
Limited retention	Data retention shall be limited to the period of the pandemic response, except for the purposes of research or epidemic planning, subject to appropriate regulation, oversight and informed consent, where required. Data used for research purposes or epidemic planning should be aggregated and anonymized where possible. Where aggregation of data is not possible for research purposes, such exceptions should be justified, and all such data should still be anonymized. Data collected for public health purposes related to COVID-19 shall be deleted following the pandemic. To the extent technically feasible, any technological system created should be dismantled at the end of the pandemic.
Infection reporting	The reporting into a digital proximity tracking application that a user has tested positive for COVID-19 could be done through several channels. In any scenario, notification of the application should require the consent of the individual. In one scenario, a user of a digital proximity tracking application could self-report an infection to the application. A health system must determine if such self-notification must be confirmed by a health professional. Alternatively, upon a patient being confirmed as positive for COVID-19, a medical professional could notify the digital proximity tracking application (with the individual's consent).
Notification	Notification of individuals who may have been in contact with a person infected with COVID-19 could, for example, be delivered directly by an application to close contacts. The notification of other users must preserve the privacy of the infected individual. Users who receive a notification through their device should receive information on the steps they should take. Such notification should be provided in clear, accessible language and explain the options that users have (including any consequences attached to these options). Such notification should be accessible to all people. This information should be provided in several languages and be accessible to people with disabilities. Users should be able to consent as to whether they wish to have the health authorities contact them for follow-up (for example, testing), including disclosure of their contact information to the health authorities. A user who has been notified by an application should not be penalized, punished or denied medical services or economic benefits for failing to follow instructions provided by the application.
Tracking of COVID-19-positive cases	After an individual who uses a digital proximity tracking application has tested positive for COVID-19, the application should not be used to track that individual's movements during his or her period of infection and recovery, including whom that individual may encounter thereafter.
Accuracy	Algorithmic models used to process data and assess risk of transmission must be reliable, verified and validated. Such applications should be open to testing by third parties and risk models should be developed with epidemiologists to establish parameters for duration and proximity before a contact is recorded and should be adjusted and improved over time. Data quality should be assessed for biases to avoid any adverse effects, including giving rise to unlawful and arbitrary discrimination.
Accountability	Any response must incorporate accountability protections and safeguards against abuse. Individuals must be given the opportunity to know about and challenge any COVID-19-related measures to collect, aggregate, retain and use data. Individuals subjected to unwarranted surveillance must have access to effective remedies and mechanisms of contestation.

Principle	Explanatory Text
Independent oversight	There should be independent oversight, including of ethical and human rights aspects, of both the public agencies and the businesses that develop, operate digital proximity tracking applications or use information obtained with them. Such oversight could include the establishment of an independent oversight body. The existence of agreements between government and business, and information necessary to assess their impact on privacy and human rights, must be publicly disclosed, along with sunset clauses and oversight. Such oversight must ensure that any use of digital proximity tracking applications by governments is firewalled from other government functions and, in the case of companies, from other business and commercial interests. An oversight body must also have access to all information necessary to ascertain that digital proximity tracking measures are necessary and proportionate to their impact and effectiveness. An oversight body should also monitor the collection and use of data to ensure they are consistent with laws and regulations and prevent abuse or exploitation of vulnerable and marginalized communities. Finally, an independent oversight body should remain in place after the end of the pandemic to ensure that any digital proximity tracking technologies that have been implemented are fully dismantled. The effectiveness of any independent oversight body depends in part on the codification and enforcement of ethical standards, human rights principles and conventions by governments, and on the respect that governments and businesses have for such principles and standards.
Civil society and public engagement	COVID-19-related responses that include data collection efforts should include free, active and meaningful participation of relevant stakeholders, such as experts from the public health sector, civil society organizations, and the most marginalized groups. This participatory approach is not only mandated from an ethics perspective – it will also enhance buy-in, voluntary participation and compliance. Furthermore, civil society can play a crucial role in holding governments and companies accountable for the deployment and operation of digital proximity tracking technologies.

References

1. Contact tracing in the context of COVID-19: interim guidance. Geneva; World Health Organization; 2020 (https://apps.who.int/iris/handle/10665/332049, accessed 21 May 2020)
2. International health regulations -- 2nd ed. Geneva; World Health Organization; 2005 (https://apps.who.int/iris/bitstream/handle/10665/43883/9789241580410_eng.pdf?sequence=1, accessed 26 May 2020)
3. Surveillance strategies for COVID-19 human infection: interim guidance. Geneva; World Health Organization; 2020 (https://apps.who.int/iris/handle/10665/332051, accessed 21 May 2020)
4. WHO guidelines on ethical issues in public health surveillance. Geneva; World Health Organization; 2017 (https://apps.who.int/iris/bitstream/handle/10665/255721/9789241512657-eng.pdf?sequence=1, accessed 7 May 2020)
5. Wong, Zoie & Zhou, Jiaqi & Zhang, Qingpeng. (2018). Artificial Intelligence for infectious disease Big Data Analytics. Infection, Disease & Health. 24. 10.1016/j.idh.2018.10.002.
6. Crocker A, Opsahl K, Cyphers B. The challenge of proximity apps for COVID-19 contact tracing. Electronic Frontier Foundation; 2020 (https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing, accessed 7 May 2020).
7. American Civil Liberties Union. Principles for technology-assisted contact-tracing. ACLU White Paper; 2020 (https://www.aclu.org/report/aclu-white-paper-principles-technology-assisted-contact-tracing, accessed 7 May 2020).
8. Parker MJ, Fraser C, Abeler-Dörner L, *et al.* Ethics of instantaneous contact tracing using mobile phone apps in the