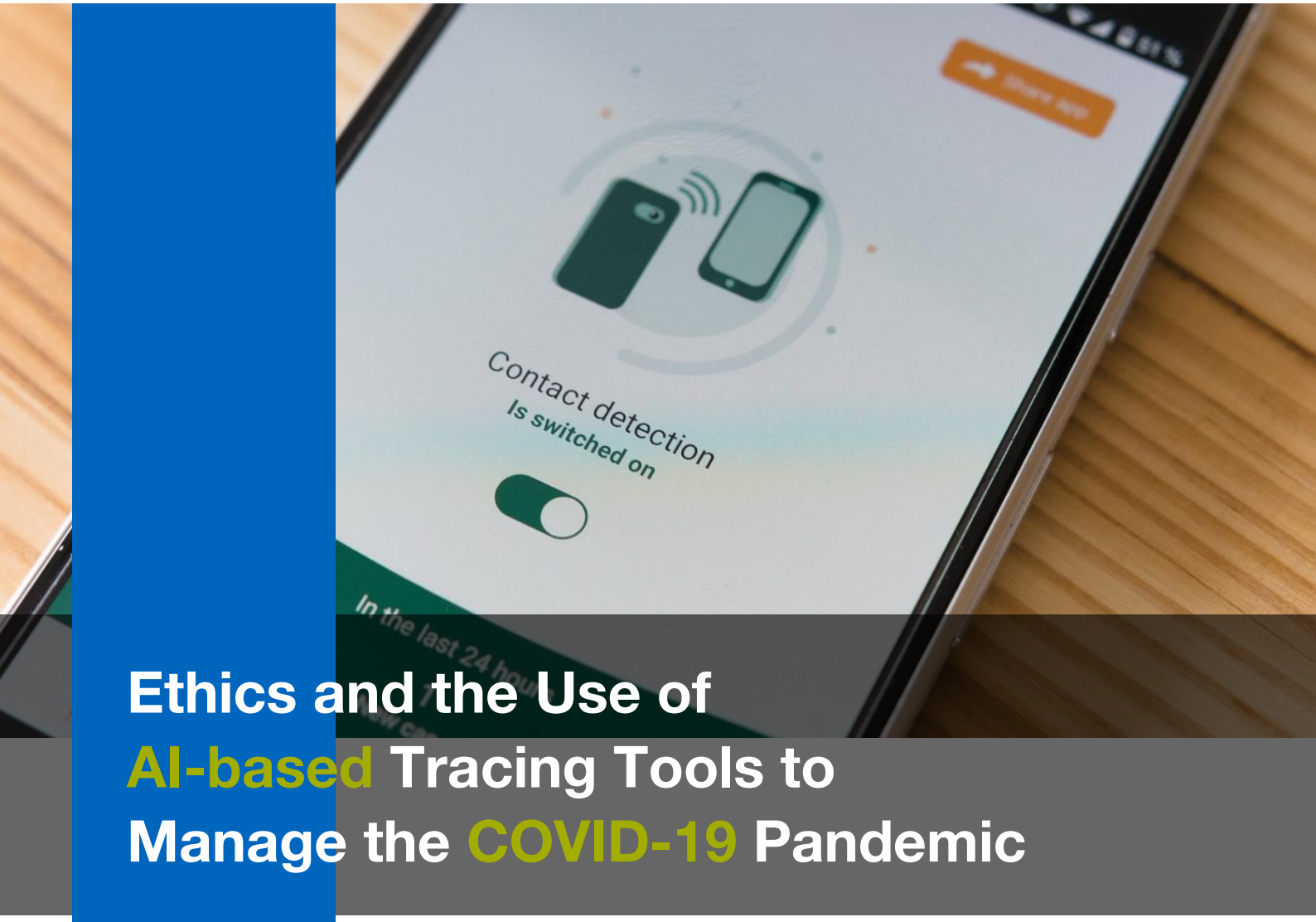
IEAI Technical University of Munich
Munich Center for Technology in Society
Institute for Ethics in Artificial Intelligence

Research Brief – June 2020



Ethics and the Use of AI-based Tracing Tools to Manage the COVID-19 Pandemic

Multiple AI-powered technologies have been developed around the world with the hope of helping to manage the COVID-19 pandemic. Traditional contact tracing methods used by healthcare workers have the potential to be complimented by AI-enabled tools. Governments around the world have moved quickly to develop approaches to digital contact or proximity tracing. The rapid development of this technology, the varying approaches to how it is employed, and its potential for widespread use, signify the urgent need to discuss not only the technological aspects of the applications, but also the ethical considerations. This brief outlines the approaches taken in some key countries, and the ethical considerations of these latest technological developments.

1. AI and Contact/Proximity Tracing Tools

In the past few months, multiple AI-powered technologies have been developed around the world with the hope of helping to manage the COVID-19 pandemic (TUM IEAI, 2020). The well-documented technique of contact tracing used by healthcare workers in previous pandemics (e.g. Ebola -WHO, 2020a-) also has the potential to be complimented by AI-based tracing methods. This process, traditionally conducted through human power, is meant to find and contact all persons at risk of having been infected by a virus, based on their previous contacts. With the evolution of AI, new solutions are being considered to improve contact tracing's effectiveness, along with questions of the ethical implications of the use of these technologies.

The main objective of an AI-powered tracing app is to alert the users who have been exposed to the virus, in order to promote testing and prevent further transmission.

The main objective of an AI-powered tracing app is to alert the users who have been exposed to the virus in some defined and significant way through mobile devices, in order to promote testing and prevent further transmission. To do so, the AI learns from one or more databases which factors are important in the spread of the virus (Kricka et al., 2020), and then tracks users based on these criteria. For example, the Mila Institute explains that based on multiple personal characteristics, health indicators, and social interactions, the Canadian COVID algorithm would be able to identify the probability for a user to be COVID-19 positive (Dilhac et al., 2020). Moreover, the machine learning process would allow the AI to build knowledge, developing its ability to predict future risk zones and understand better how the virus spreads.

There are limitations to this approach as well. The World Health Organization (WHO), for instance, proposes a distinction between contact tracing and proximity tracking since, when using the app-based technology, mobile devices evaluate the distance between individuals according to the strength of the signal between them (WHO, 2020b). The technology, therefore, lacks situational details (e.g. were those individuals wearing masks, did the user touch an object that was carrying the virus, etc.) and relies only on proximity-related information (Kricka et al., 2020). This distinction displays the potential limitations of relying purely on technological solutions and suggests instead the need to use them in conjunction with other more traditional pandemic management responses.

In terms of the technology, the two main questions revolve around how to determine proximity and how to transmit and store data. To evaluate the proximity between humans, research groups have united mainly along a similar approach. The TraceTogether team from Singapore, the European consortium Decentralized Privacy-Preventing Proximity Tracing (DP-3T) and the MIT in Cambridge Private Automated Contact Tracing (PACT) group advocated the use of Bluetooth's signal (PACT, 2020; TraceTogether, 2020; Troncoso, C. et al., 2020; Zastrow, 2020a). The device used would generate a new broadcasted identity number several times a day in an effort to preserve the anonymity of the user. Every code previously generated by an individual's device is registered on the surrounding people's devices, alongside information on the strength of the signal. In the case of a user contracting COVID-19, the individual can enter the information into the app. All the generated identification codes are then downloadable and checked by other users, allowing them to be aware of the situation, and to make decisions accordingly (Leins et al., 2020).

In another less popular contact/proximity tracing option, movements are tracked through phone location data (e.g. GPS signal) and compared with other users' data, in order to reach similar conclusions as the ones presented earlier (Howell O'Neill et al., 2020).

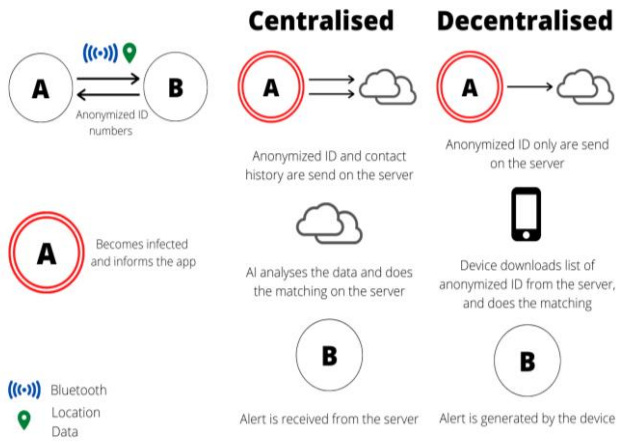


Figure 1 - Technology of centralised/decentralised and GPS/Bluetooth approaches

In terms of data transaction and storage, centralized and decentralized models have been identified (Figure 1). In a centralized mode, anonymized data is uploaded to a central server where algorithms are run to determine risks of infections for each individual. A unique anonymous number is then given by the server to each individual, pending authorization from the COVID-infected users to share their data. In the decentralized approach, users keep their information on their devices and decide whether to share it with others – specifically if the user is tested positive to COVID-19, allowing users to have more control over their personal information (Criddle & Kelion, 2020).

Companies and governments have varying opinions on the best models. Apple and Google, for instance, support the decentralized approach and proposed a model that resolved previous technical issues encountered concerning the Bluetooth data sharing from iPhones to other devices.[1] Some governments, like the United Arab Emirates, advocate a mixed model app in which users will keep their data in their phones, but might be asked to give access to the government if deemed necessary (TraceCovid app). Table 1 provides an overview of the approaches being employed in different countries.

The rapid development of this technology, the varying approaches to how it is employed, and its potential for widespread use, signify the need to discuss not only the technological aspects of the applications, but also the ethical considerations. Issues of privacy, effectiveness, accessibility and transparency, among others, are already being debated by various stakeholders. This Research Brief outlines the approaches taken in some key case study countries, and the ethical considerations of these latest technological developments.

Table 1: Overview of proximity tracing apps approach by country[2]

	Location	Bluetooth
Centralized	China**; Qatar*; Russia; South Korea; India*; Turkey*; Bahrain; Kuwait; Norway*; Bulgaria; Algeria**; New Zealand**	Australia; Singapore; France; Mexico; Fiji; Tunisia
Decentralized	Israel; Jordan	Italy; Germany; Japan; Finland; United Kingdom; Poland; Austria; Canada; Ireland; Switzerland; North Macedonia; Malaysia; Estonia; United Arab Emirates; Hungary, Latvia, Spain

* Use both location and Bluetooth data
**Includes QRcode Scanning

2. Approaches to AI and the Use of Contact Tracing - Country Comparison

Countries around the world have developed or are developing different solutions to manage COVID-19. However, technological development and its use does not take place in a vacuum. The use and acceptance of new technologies are linked to the social and political environments where they are employed. Political openness, as well as previous experience with intrusive technology (See Table 2), are important determinants of the approaches countries use for contact/ proximity tracing apps. Thus, our comparative examination of countries' approaches groups their responses along these factors. The countries we examine provide clear examples of varied approaches to contact/proximity tracing app development and use, giving insight into the potential ethical considerations for these technologies.

[1]Both companies will release APIs that enable interoperability between Android and iOS devices using apps from public health authorities (Apple Organisation, 2020).

[2]Howell O'Neill et al., 2020 and European Commission, 2020. For more comprehensive and detailed list see Appendix 1.

Table 2: Case study countries' governance and surveillance technology experience

Country	Political Openness[3]	Experience with Intrusive Technology[4]
Australia	High (1.43)	Low/Moderate
Germany	High (1.42)	Low
Italy	High (1.05)	Low
Norway	High (1.70)	Low
Israel	Moderate (0.65)	Moderate/High
South Korea	Moderate (0.79)	Moderate/High
Singapore	Moderate/Low (-0.06)	Moderate/High
Qatar	Low (-1-20)	High
Russian Federation	Low (-1.06)	High
China	Low (-1.44)	High

2.1 High Levels of Political Openness, Limited Experience with Surveillance technology

The **German** Corona-Warn-App (Open-Source Project Corona-Warn-App) and its development provide a clear case study of the approach of a country with high political openness and societal aversion to surveillance technology. Developed mainly by SAP SE and Deutsche Telekom AG, the app was proposed by the German government as a part of their Trace and Test strategy against the spread of COVID-19. After discussion of centralizing the data, the government decided to go with a decentralized approach, using the Google/Apple API (Corona-Warn App · GitHub). Data collection is limited to the strict minimum, and all data sharing by users is pending voluntary and informed approval. As a later development, a team of the Technical University of Munich (TUM) proposed QRONITON, a voluntary QR code scanning solution to help with the registration of individuals in certain public places and contact tracing while protecting the users' data (Carle, 2020). When scanning the code, a timestamped phone number of the user and postal code will be sent to a central server in a highly encrypted form. If a user is tested positive, a digital code will be sent to the user to enter in QRONITON if they are willing to let governmental institutions access their travel history. Keeping accessibility at a high level, the technology allows for printing out of personal QR codes, scan-able by the places visited. Together, the tracing app and the QR code solution are presented as two sides of the same coin in the prevention of coronavirus spread. The emphasis on decentralized data collection, code-transparency and voluntary use is not surprising given the environment in which the app will be used.

Adopting a quite similar approach for its tracing app (Amante et al., 2020), **Italy's** Immuni integrity was questioned as it has been developed by Bending Spoons, a company partially financed by Chinese investors (Coronavirus, Immuni, 2020). To tackle the possible ensuing mistrust, the company published the technical specifications and images of the app (Immuni documentation).

With another data storage approach, **Australia** proposed COVIDSafe (Australian Government Department of Health, 2020). The app registered 5.3 million users on May 11th, 2020. Using Bluetooth technology, Australia decided to centralize the users' data on an Amazon Cloud Service (Taylor, 2020b). Acknowledging a possible reticence to using the app due to the lack of data protection clarity, the parliament passed a Privacy Amendment (Public Health Contact Information) on May 14th, 2020. Moreover, the Australian authorities shared the app code for public consultation (AU-COVIDSafe). The users that test positive for COVID-19 can inform the app and are asked to agree to share their data. If they agree, all contact events within the past 21 days are uploaded onto the central server under the user's individually generated ID number (Greenleaf & Kemp, 2020; Taylor, 2020a). The Australian government confirmed that a data destruction plan is in place.[5]

[3] Numbers taken from 2018 recordings of governance indicators from Kaufmann, Kraay and Mstruzzi (2010)

[4] Based on known government use of tracking technology in other sectors or for past purposes.

[5] An ethical challenge arose from this data storage setting - Through the user's ID number, the authorities can monitor the user's app activity in the past 2 hours (Leins et al., 2020). There has not yet been a technological response.

Italy and Australia provide insightful cases of how politically open systems have had to adapt to public concerns regarding privacy and transparency in order to increase potential use, even at the possible detriment to virus containment effectiveness.

*Country Snapshot: **Norway** launched Smittestopp in mid-April, becoming one of the first countries to do so (Kelion, 2020). Using Bluetooth and location data collection in a centralized manner, the app was deemed "one of the most alarming mass surveillance tools" by Amnesty International (Anderson, 2020). Due to these concerns, Norway interrupted the spread of its app and reviewed its data privacy elements to ensure safer storage.*

2.2. Moderate Levels of Political Openness, Some Experience with Surveillance Technologies

South Korea provides an interesting case where surveillance methods already in place and initially used to find tax evaders and track criminals were repurposed (using credit and debit card transaction, phone location logs, and surveillance camera images) (Cellan-Jones, 2020). There is a precedent for this in South Korean law regarding data privacy when it comes to infected citizens (Stanley & Granick, 2020). The modifications in the law, allocating more power to investigators, were established after the 2015 Middle East Respiratory Syndrome (MERS) episode (Bicker, 2020). Using the already-in-place technology, data are anonymized, and a COVID-19 positive patients' location history is published on the Ministry of Health and Welfare website. Citizens living in the defined zone of the patient's activities are notified by a text on their phones sent by the government. South Korea has then put a focus on making testing as available and fast as possible for those who received alerts (COVID-19: Lessons from South Korea, 2020).

As a consequence of such explicit messages and their privacy implications, fear of being tested at all arose in the population. To deal with this, the South Korean government announced that sharing personal information will now be only the last resort, if the mapping of the individuals' interactions was not doable otherwise (Zastrow, 2020b).

*An example of a message from the **South Korean** Government: « A 43-year-old man, resident of Nowon district, tested positive for coronavirus, He was at his work in Mapo district attending a sexual harassment class. He contracted the virus from the instructor of the class » (Coronavirus privacy, 2020).*

Israel provides a similar case of repurposing practices already in place. The government reacted quickly to the COVID-19 outbreak. By mid-March, under emergency powers, they allowed the implementation of smartphone location tracking for the people considered infected. Those individuals, and the ones deemed at risk to be infected, were then ordered to quarantine (Sachs & Huggard, 2020). Shin Bet, the Israeli Security Agency, was put in charge of the contact/proximity tracing effort. The technology used was familiar to them as the system and database were initially developed for counterterrorism purposes (Howell O'Neill, 2020). At the time, the country's supreme court of justice vocalized its concern for privacy violations, pushing back the execution of the tracing system (Leiba, 2020). In the end, Shin Bet was finally allowed to use phone data – notably cell tower connection, to trace back infected civilians' movements under restricted data collection, but without having to answer to the freedom of information laws (Gross, 2020; Stanley & Granick, 2020). Regardless, the HaMagen app (HaMagen – The Ministry of Health App for Fighting the Spread of Coronavirus) was launched by the Health Ministry to help in the contact/proximity tracing effort. Citizens have the choice to use it or not. The app uses a decentralized approach, collecting a limited number of location data and has transparent coding (MohGovIL).

*Country Snapshot: While **Singapore** rates low on political openness, they have taken a strongly privacy-preserving and voluntary approach to contact/proximity tracing. This may be related to the fact that Singapore has been proactive in developing frameworks for AI governance (PDPC, 2020). The TraceTogether app was the first major tracing app, recruiting 1,500,000 users in the first weeks (TraceTogether). The app uses a Bluetooth (Bluetrace) technology, centralizing the data, coupled with QR codes to scan at the entrance of vulnerable places (Kricka et al., 2020). However, since much of the virus spread is among foreign workers, accessibility of the app and language barriers are a serious hindrance to its effectiveness (Zastrow, 2020a). As a partial solution, wearable devices will be available to residents not owning the device necessary for the app (Baharudin, 2020).*

2.3 Low Levels of Political Openness, Experience with Surveillance Technology

More drastic approaches have been observed mainly in countries with low levels of political openness and a history of surveillance in other sectors. In the most discussed example, China, the Ministry of Information Industry Technology developed a contact/proximity tracing app assigning a color to the citizens: red goes for 14 days in quarantine, yellow for 7 days in quarantine, and green for no quarantine. When entering a public place, users are asked to scan a QR code. Depending on the user's color, authorities will be alerted of a potential quarantine breach. While the app is used on a voluntary basis, it is required to enter certain public places. The system behind the app is probably based on localization, but the app code is not public, and therefore this information cannot be confirmed. Moreover, data collected through the app and other technologies do not require consent to be shared according to the Chinese National Health Committee. Authorities are also using other already-in-place technology to monitor citizens, including CCTV and credit card history. However, it is important to highlight that regional differences exist in the app. For example, Beijing's app indicates that data collection is compliant with the law, and only for COVID-19 purposes. However, it is as of yet unclear who can access the app and how the data will be used (Gamvros, et al., 2020).

In another noteworthy case, **Russia** developed further mandatory tracing technologies to deal with the pandemic. A patient-tracking app in Moscow ensures that coronavirus patients stay at home. In this case, patients' data are said to be erased after the treatment is completed (Chislova, 2020). Digital travel permits with QR codes regulate transportation (car or public) of citizens, depending on the authorizations given through company status or personal requests. Finally, the federal tracing system allows authorities to instruct mobile networks to inform individuals, or remind them, to self-isolate, and to monitor their GPS location data.

*Country Snapshot: Amnesty International called **Kuwait's** « Shlonik » the most invasive app, with a low privacy for the users, and a low security of the data (Anderson, 2020). Use of the app was linked to participation in a TV show, where users who were known via the app to be at home during Ramadan were offered prizes.*

In a final example, **Qatar's** Ministry of Digital Affairs developed Ehteraz, a centralized-model contact/proximity tracing app, mandatory for residents. This system uses Bluetooth and location technology, requiring further access to the photos on the user's device. Data is stored on a central server with the name, national ID, health status and location data of about a million citizens. The government has not announced a data destruction plan yet, and the app code has not been made public (EHTERAZ app). On May 21st, 2020,

Amnesty International found a privacy vulnerability on the central server used to store those data. The Qatari government quickly fixed the cybersecurity issue, but the information of a million users were reachable for an unknown period of time (*Qatar: Contact tracing*, 2020).

3. Ethical Considerations in the Use of Contact/Proximity Tracing Apps

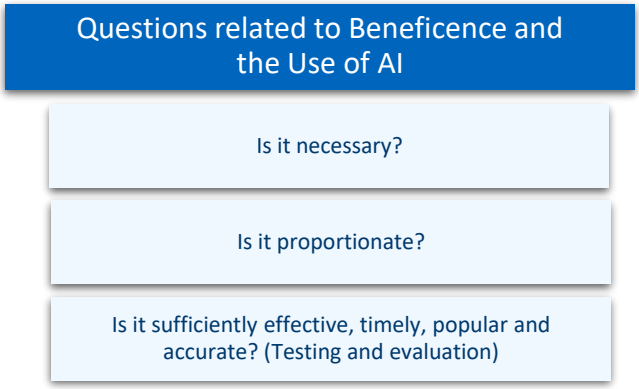
The above analysis demonstrates clearly that AI-based tracing apps are being employed widely and in a variety of forms. Preferred technical approaches are related to the forms of governance in the given environment, as well as historical experience with intrusive technologies. However, alongside this emergence is a varying degree of concern from governments, developers and the public on the ethical considerations related to the apps' use. How might the app violate personal privacy, and how do we make sure these violations are proportionate to the public health gains it generates? How do we make sure the data it generates are used only for intended purposes? And is access to the technology equitable and unbiased?

The WHO and researchers from Oxford University have released largely overlapping ethical guidelines for the implementation of COVID-19 tracing apps (WHO, 2020; Morley et al. 2020). Moreover, the European Union Commission (CNECT, 2020) issued recommendations with regard to the data protection and the app development. The WHO reminded the member states of their obligation to develop technology complying with the International Health Regulations, ensuring the transparency of the data collection system, and the protection of those data. The EU Commission complemented these statements by reminding EU member states of existing laws surrounding surveillance, and reaffirming the responsibility of state's health authority regarding the privacy rights of civilians. The IEAI aims to build upon this discussion by putting their findings explicitly in the context of an *AI ethics framework*. We build this reflection based on the AI4People's work (Floridi et al. 2018), which first proposed the five principles (later adopted by the European HLEG on AI) to guide AI ethics: **Beneficence, Non-Maleficence, Autonomy, Justice** and **Explicability**. Within each principle, we outline proposed guidelines/ethical questions related to AI-enabled contact/proximity tracing and discuss their relation to AI ethics.

3.1 Beneficence

Beneficence can be described as promoting well-being, preserving dignity, and sustaining the planet, or, in short, 'do only good'. A major consideration, therefore, related to tracing apps is whether and how they are providing benefit in terms of managing the spread of COVID-19. As the WHO (2020) also argues, if we are considering the tradeoffs between the potential issues related to non-maleficence (below) and public health gains, the accuracy, proportionality, and effectiveness of the app is a valuable indicator. Thus, testing and evaluation of the impacts of the app will be of vital importance.

Too many false positives or negatives could lead to unjustified overreliance on the app or lack of use due to the appearance that it is providing too many false positives (Morley et al., 2020).

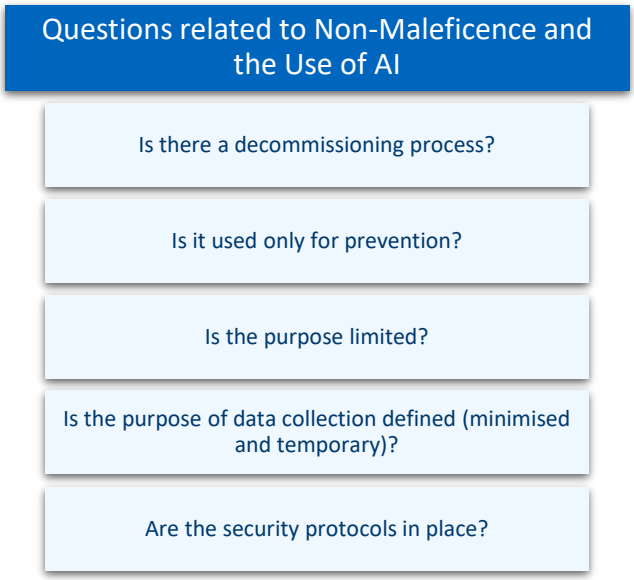


3.2 Non-Maleficence

Non-maleficence implies 'do no harm'. Both the centralized and decentralized approaches to proximity tracing involve privacy and cybersecurity concerns that could affect individual users. A centralized approach makes an easier target for data hacking because each user carries a specific anonymized ID. Moreover, in terms of privacy, in a centralized system, there is no clear assurance of the destruction of unneeded data by authorities, or at least this might be a perception of the public.

This could lead to a lower engagement in the use of the app (where voluntary), making it less effective. On the other hand, a decentralized approach might open the door to trolls, creating anxiety for users in the case of false positive.

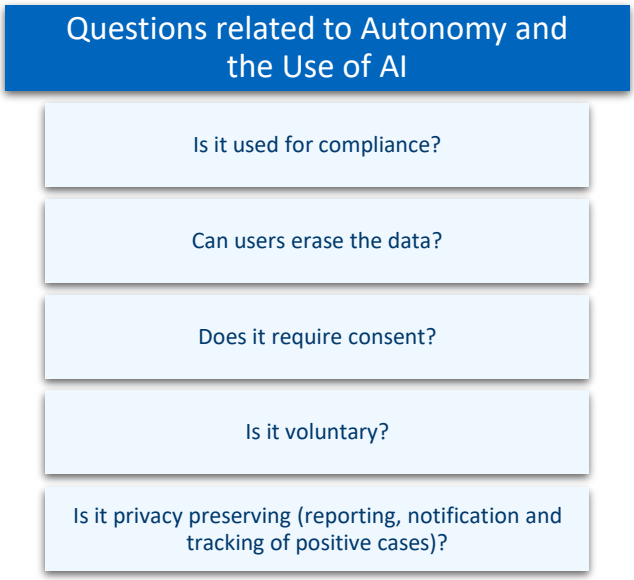
Moreover, there is the underlying risk of mission creep or unintended use of collected data. Thus, many of the ethical considerations related to the app and non-maleficence focus on the limitation of time and purpose, as well as anonymity assurances.



Issues concerning non-maleficence relate clearly to other ethical principles. If the reduction of potential harms is not addressed, trust in the technology will be limited, and in the case where use of the applications is voluntary, this will reduce uptake and overall effectiveness (lowering the "beneficence" criteria of the application).

3.3. Autonomy

Autonomy encompasses the idea that individuals have the right to make decisions for themselves.[6] This already calls into question the non-voluntary use of AI-based tracing and underlines the importance of garnering individual consent at several steps along the way (tracing, reporting, notifying) and providing mechanisms for data deletion. The German Corona-Warn app provides an example of this, where users must provide consent within the app for various tasks, including enabling Bluetooth tracking, uploading results and dealing with notifications, as well as clear instructions for toggling these functions off and offloading the app.



3.4 Justice

Justice deals with shared benefits and shared prosperity and relates to the distribution of resources and eliminating discrimination. As Morely et al. (2020) mention, some apps are not available for older operating systems. Moreover, how can we address the issue of equitable access for sections of the population who are less likely to have smartphones altogether, such as the elderly or the homeless. This is a particularly distressing issue as it coincides with the populations already more at risk for complications due to the virus.

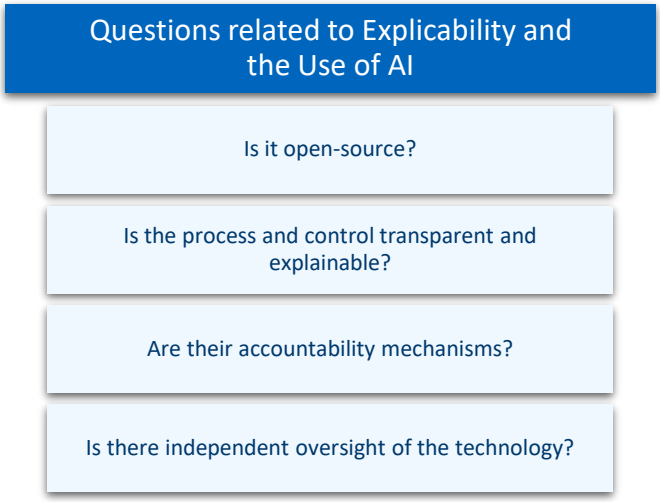
Moreover, as has already been discussed, trust in technology is essential if we want to arrive at the level of usage needed to improve the effectiveness of the app. Therefore, buy-in from the community, through public engagement in the development and implementation process, is a worthwhile consideration to not only make the ethical tradeoffs more transparent, but also to improve the justice and beneficence criteria, thus making the tradeoffs less dramatic. Relatedly, we have added the

[6] This issue is also particularly of note as it relates to AI and human rights (Kriebitz &Lütge, 2020).

question of whether the app is *equally* impactful. This is related to the need for evaluation and testing to determine effectiveness (beneficence) and to the question whether the app is more effective in preventing virus spread in certain populations compared to others, which could be related to accessibility issues or algorithmic bias. The example of the suggested use of tracing bracelets in Singapore displays the known need to confront this issue.

3.5 Explicability

Explicability is an additional concept that focuses on enabling the other principles through making explicit the need to understand and hold to account the AI decision-making processes. In our April brief (IEAI, 2020), we questioned where issues of explicability would rank in the rush to develop technology to deal with a crisis as urgent as the COVID-19 pandemic. In this case, however, since the usefulness of the app as a pandemic management tool depends on a significant amount of the population opting in to use it (at least in the case of voluntary use), building trust in the technology is of the utmost importance. Knowledge and transparency have arguably been linked to improving trust (Albinson et al., 2019; Cook et al., 2010; Sanders et al., 2014 - among others).[7] Explicability is, therefore, a key issue in this particular case.



As noted above, these principles are interrelated, as are the questions associated with them. For example, explicability helps with efficacy (beneficence) because it will increase the uptake of usage that is necessary for increasing the effectiveness of the app. It is also related to justice because, in order to provide mechanisms for accountability and public engagement, those stakeholders need to have access to information and understand what the app is doing and how. The example of the German Corona-Warn app and its open source coding available on Github is an example of how transparency can be made a priority and realized. Whether this will lead to significantly higher uptake of usage is still unclear as of the time of writing.

4. Final Thoughts

Given the variations in approaches that countries have taken to AI-enabled contact/proximity tracing and the rate at which new apps are being released, it is important to consider the ethical consequences of these approaches now. By viewing the potential ethical questions through an *AI ethics framework,* we are able to understand potential issues with respect to the technology in particular and compare it with issues encountered with other AI-based technologies. Perhaps providing guidance from solutions that have worked in other context. What is also clear is that an overall strategy for managing the spread of COVID-19 is

[7] Although, notably for our comparative approach to this topic, the prioritization of transparency to enhance public trust can vary between societies (Grimmelikhuijsen et al., 2013).

needed. One that incorporates new technological approaches into tracing, but also utilizes other policy and public health interventions (WHO, 2020). Moreover, as our comparative analysis of the use of these tools shows, what may be effective in one context may engender distrust or create inaccuracies in another environment. Thus, a comparative analysis of the use of contact/proximity tracing technology that takes into account societal, political and environmental circumstances and implications will be useful going forward as policymakers look to lessons learned, successes and failures.

This brief serves as a starting point for a longer comparative study the IEAI is developing, with partners from the Global AI Ethics Consortium (GAIEC).

5. References

Albinson, N., Balaji, S., & Chu, Y. (2019, September 23). *Building digital trust: Technology can lead the way.* Deloitte Insights. https://www.deloitte.com/us/en/insights/topics/digital-transformation/building-long-term-trust-in-digital-technology.html

Amante, A., Pollina, E., Jones, G., & Elgood, G. (2020, June 1). *Italy launches COVID-19 contact-tracing app amid privacy concerns*. Reuters Technology News. https://www.reuters.com/article/us-health-coronavirus-italy-app/italy-launches-covid-19-contact-tracing-app-amid-privacy-concerns-idUSKBN2383EW

Anderson, I. (2020, June 16). *Coronavirus: Alarm over "invasive" Kuwait and Bahrain contact-tracing apps.* BBC News. https://www.bbc.co.uk/news/amp/world-middle-east-53052395

Apple Organisation. (2020, May 20). *Apple and Google partner on COVID-19 contact tracing technology*. Apple Newsroom. https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

Coronavirus privacy: Are S Korea virus alerts too revealing? (2020, March 5). BBC News. https://www.bbc.com/news/world-asia-51733145

Australian Government Department of Health. (2020, June 3). *COVIDSafe app*. https://www.health.gov.au/resources/apps-and-tools/covidsafe-app#get-the-app

Baharudin, H. (2020, June 15). *Apple-Google contact tracing system not effective for Singapore: Vivian Balakrishnan*. The Straits Times. https://www.straitstimes.com/singapore/apple-google-contact-tracing-system-not-effective-for-singapore-vivian-balakrishnan

Bicker, L. (2020, March 12). *Is S Korea's rapid testing the key to coronavirus?* BBC News. https://www.bbc.com/news/world-asia-51836898

Carle, G. (2020, June 12). *Contact tracing while protecting privacy*. TUM, COVID-19, Research News. https://www.tum.de/nc/en/about-tum/news/press-releases/details/36066/

Cellan-Jones, R. (2020, May 15). *Tech Tent: What can we learn from South Korea?* BBC News. https://www.bbc.com/news/technology-52681464

Chislova, O. (2020, May 13). *Contact tracing apps: Russia is different*. Freshfields Bruckhaus Deringer. https://digital.freshfields.com/post/102q74r/contact-tracing-apps-russia-is-different

CNECT: Directorate-General for Communications Networks, Content and Technology, & COM: European Commission. (2020, April 8). *Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*. Publication Office of the European Union. ,https://op.europa.eu/en/publication-detail/-/publication/1e8b1520-7e0c-11ea-aea8-01aa75ed71a1/language-en

Cook, F. L., Jacobs, L. R., & Kim, D. (2010). *Trusting what you know: Information, knowledge, and confidence in Social Security*. The Journal of Politics, 72(2), 397-412.

Coronavirus, Immuni: i finanziamenti dalla Cina e il rischio che i dati italiani finiscano in mani straniere. (2020, April 20). Lastampa.It Top News. https://www.lastampa.it/topnews/primo-piano/2020/04/21/news/coronavirus-immuni-i-finanziamenti-dalla-cina-e-il-rischio-che-i-dati-italiani-finiscano-in-mani-straniere-1.38742253

COVID-19: Lessons from South Korea. (2020, June 9). Health Systems Global. https://healthsystemsglobal.org/news/covid-19-lessons-from-south-korea/

Criddle, C., & Kelion, L. (2020, May 7). *World split between two types of virus tracing app*. BBC News. https://www.bbc.com/news/technology-52355028

Dilhac, M.-A., Bengio, Y., Rish, I., Janda, R., Ghosn, J., Borreman, S., Pisano, V., & Prud'homme, B. (2020, May 23). *COVI : Une application de suivi de contacts intelligente…et éthique*. Mila Institut Quebec. https://mila.quebec/covi-une-application-de-suivi-de-contacts-intelligenteet-ethique/

European Commission. (2020). *ANNEX IV: INVENTORY MOBILE SOLUTIONS AGAINST COVID-19* (No. 4). ec.europa.eu. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_annex_en.pdf

Floridi, L., Cowls J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Lütge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P. & Vayena, E. (2018). *AI4People – An ethical framework for a good society: opportunities, risks, principles, and recommendations*. Minds and Machines, 28(4), 689-707.

Gamvros, A., Cwalina, C., Evans, M., & Flockhart, F. (2020, May). *Contact tracing apps in China*. Norton Rose Fulbright. https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/contact-tracing/china-contact-tracing.pdf?revision=249d55f4-eb9a-49dd-8491-b8c9c7626691&la=en-ru

Greenleaf, G. & Kemp, K. (2020, May 15). Australia's COVIDSafe Experiment, Phase III: Legislation for Trust in Contact Tracing. *University of New South Wales Law Research Series*. http://dx.doi.org/10.2139/ssrn.3601730

Grimmelikhuijsen, S., Porumbescu, G., Hong, B., & Im, T. (2013). *The effect of transparency on trust in government: A cross-national comparative experiment.* Public Administration Review, 73(4), 575-586.

Gross, J. A. (2020, March 15). *Government okays mass surveillance of Israelis' phones to curb coronavirus*. The Times of Israel. https://www.timesofisrael.com/government-okays-mass-surveillance-of-israelis-phones-to-curb-coronavirus/

Howell O'Neill, P. (2020, May 7). *India is forcing people to use its covid app, unlike any other democracy*. MIT Technology Review. https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-app-mandatory/

Howell O'Neill, P., Ryan-Mosley, T., & Johnson, B. (2020, May 7). *A flood of coronavirus apps are tracking us. Now it's time to keep track of them.* MIT Technology Review. https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/

Kaufmann, D., Kraay. A. and Mastruzzi, M. (2010). *The Worldwide Governance Indicators: Methodology and Analytical Issues*. World Bank Policy Research Working Paper No. 5430. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1682130 (Data Retrieved 19 June 2020).

Kelion, L. (2020, June 15). *Covid-19 contact-tracing app forced to delete data*. BBC News. https://www.bbc.com/news/technology-53051783

Kricka, L. J., Polevikov, S., Park, J. Y., Fortina, P., Bernardini, S., Satchkov, D., Kolesov, V. & Grishkov, M. (2020). *Artificial Intelligence-powered search tools and resources in the fight against COVID-19*. EJIFCC, 31(2), 106.

Kriebitz, A. & Lütge, C. (2020). *Artificial Intelligence and Human Rights: A Business Ethics Assessment.* Business and Human Rights Journal, 5, pp. 84-104.

Leiba, O. (2020, March 23). *Hamagen - Fight Coronavirus and Preserve Privacy*. Medium. https://medium.com/@oleiba/hamagen-fight-coronavirus-and-preserve-privacy-b1631693bb46

Leins, K., Culnane, C., & Rubinstein, B. I. (2020). *Tracking, tracing, trust: contemplating mitigating the impact of COVID-19 through technological interventions*. The Medical Journal of Australia, 1.

Qatar: Contact tracing app security flaw exposed sensitive personal details of more than one million. (2020, May 26). Amnesty International. https://www.amnesty.org/en/latest/news/2020/05/qatar-covid19-contact-tracing-app-security-flaw/

Morley, J., Cowls, J., Taddeo, M., & Floridi, L. (2020, June). *Ethical guidance for COVID-19 tracing apps*. Nature, 582, 29-31.*PACT: Private Automated Contact Tracing*. (2020). PACT: Private Automated Contact Tracing. https://pact.mit.edu/

Personal Data Protection Commission, Singapore (PDPC). (2020, January). *Model Artificial Intelligence Governance Framework, Second Edition*. Singapore Government.

Sachs, N., & Huggard, K. (2020, June 10). *Technosurveillance mission creep in Israel's COVID-19 response*. Brookings. https://www.brookings.edu/techstream/technosurveillance-mission-creep-in-israels-covid-19-response/

Sanders, T. L., Wixon, T., Schafer, K. E., Chen, J. Y., & Hancock, P. A. (2014, March). *The influence of modality and transparency on trust in human-robot interaction*. In 2014 IEEE International Inter-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 156-159.

Stanley, J., & Granick, J. S. (2020). *The limits of location tracking in an epidemic*. American Civil Liberties Union.

Taylor, J. (2020a, May 2). *Coronavirus apps: how Australia's Covidsafe compares to other countries' contact tracing technology*. The Guardian. https://www.theguardian.com/australia-news/2020/may/03/coronavirus-apps-how-australias-covidsafe-compares-to-other-countries-contact-tracing-technology

Taylor, J. (2020b, May 15). *Covidsafe app: how Australia's coronavirus contact tracing app works, what it does, downloads and problems*. The Guardian. https://www.theguardian.com/australia-news/2020/may/15/covid-safe-app-australia-how-download-does-it-work-australian-government-covidsafe-covid19-tracking-downloads

TraceTogether. (2020). Singapore Government Agency Website. https://www.tracetogether.gov.sg/

Troncoso, C. et al. (2020, April 19). *DP3T - Decentralized Privacy-Preserving Proximity Tracing*. GitHub. https://github.com/DP-3T/documents

TUM Institute for Ethics in Artificial Intelligence (IEAI). (2020, April). *Ethical Implications of the Use of AI to Manage the COVID-19 Outbreak* (No. 2). https://ieai.mcts.tum.de/wp-content/uploads/2020/04/April-2020-IEAI-Research-Brief_Covid-19-FINAL.pdf

World Health Organization (WHO). (2020a, February 17). *WHO strategic response plan 2015: West Africa Ebola outbreak*. https://www.who.int/csr/resources/publications/ebola/ebola-strategic-plan/en/

World Health Organization (WHO). (2020b, May 28*). Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing: interim guidance*. https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1

Zastrow, M. (2020a, May 19). *Coronavirus contact-tracing apps: can they slow the spread of COVID-19?* Nature. https://www.nature.com/articles/d41586-020-01514-2?error=cookies_not_supported&code=97fb9442-298c-4b01-b27c-ee660eb4c01d

Zastrow, M. (2020b, March 18). *South Korea is reporting intimate details of COVID-19 cases: has it helped?* Nature. https://www.nature.com/articles/d41586-020-00740-y?error=cookies_not_supported&code=0d786d82-60a6-4cc3-a364-44c2b30ca5e4

6. Appendices

Appendix 1 – Detailed overview of proximity tracing apps approach by country

Country	App	Technology Used	Data Solution	Voluntary / Mandatory
Algeria	Covid Rescue	QR code Scanning	Centralized	Voluntary
Australia	COVIDSafe	Bluetooth	Centralized	Voluntary
Austria	Stopp Corona	Bluetooth	Decentralized	Voluntary
Azerbaijan	e-Tabib	Bluetooth	?	Voluntary
Bahrain	BeAware	Bluetooth	?	?
Bangladesh	Corona Tracer BD	Bluetooth	?	?
Bulgaria	ViruSafe	Location	Centralized	Voluntary
Canada	COVID Alert	Bluetooth	Decentralized	Voluntary
China	Chinese health code system	Location	Centralized	Mandatory
Columbia	CoronApp	Bluetooth	?	?
Cyprus	CovTracer	Location, GPS	?	Voluntary
Czech	eRouska	Bluetooth	?	Voluntary
Estonia	Estonia's App	Bluetooth	Decentralized	Voluntary
Fiji	CareFiji	Bluetooth	Centralized	Voluntary
Finland	Ketju	Bluetooth	Decentralized	Voluntary
France	StopCovid	Bluetooth	Centralized	Voluntary
Germany	Corona-Warn-App	Bluetooth	Decentralized	Voluntary
Ghana	GH COVID-19 Tracker	Location	?	Voluntary
Hungary	VìrusRadar	Bluetooth	Decentralized	Voluntary
Iceland	Rakning C-19	Location	?	Voluntary
India	Aarogya Setu	Bluetooth, Location	Centralized	Mandatory
Iran	Mask.ir	Location	?	Voluntary
Ireland	HSE Covid-19 App	Bluetooth	Decentralized	Voluntary
Israel	HaMagen	Location	Decentralized	Voluntary
Italy	Immuni	Bluetooth	Decentralized	Voluntary
Japan	COCOA	Bluetooth	Decentralized	Voluntary
Jordan	AMAN App - Jordan	Location	Decentralized	?
Kuwait	Shlonik	Location	Centralized	?
Latvia	Apturi Covid	Bluetooth	Decentralized	Voluntary
Malaysia	MyTrace	Bluetooth	Decentralized	Voluntary
Mexico	CovidRadar	Bluetooth	Centralized	Voluntary
New Zealand	NZ COVID Tracer	QR code Scanning	Centralized	Voluntary
North Macedonia	StopKorona	Bluetooth	Decentralized	Voluntary
Norway	Smittestopp	Bluetooth, Location	Centralized	Voluntary
Poland	ProteGO	Bluetooth	Decentralized	Voluntary
Qatar	Ehteraz	Bluetooth, Location	Centralized	Mandatory

Singapore	Trace Together	Bluetooth	Centralized	Voluntary
Spain	OpenCoronavirus	Bluetooth	Decentralized	Voluntary
Switzerland	Swiss Contact Tracing App	Bluetooth	Decentralized	Voluntary
Tunisia	E7mi	Bluetooth	Centralized	?
Turkey	Hayat Eve Sığar	Bluetooth, Location	Centralized	Mandatory
United Kingdom	NHS COVID-19 App	Bluetooth	Decentralized	Voluntary
United Arab Emirates	TraceCovid	Bluetooth	Decentralized	Voluntary

Note: "?" indicates that the approach is not been made publically clear at this time.
List complied from: Howell O'Neill et al., 2020