# A Human Centric Framework to Evaluate the Risks Raised by Contact-Tracing Applications

Beatriz Botero Arcila

# A Human Centric Framework to Evaluate the Risks Raised by Contact-Tracing Applications[1]

**By Beatriz Botero Arcila[2]**

## 1. Introduction

Digital technologies and data-gathering and analytics are gaining prominence in the strategies adopted by governments all over the world as they address many of the challenges associated with the Covid-19 pandemic. Contact-tracing applications, in particular, promise to help contain the spread of the virus and allow societies to slowly relax social distancing measures. However, digital solutions pose a variety of risks to the security of individuals, and the enjoyment of human rights. This document proposes a framework to analyze how technical design and governance interplay in contact-tracing applications and how this interplay balances the safety needs of individuals and society at large. The document focuses on the two most prominent models at the time of writing, the Google-Apple protoco, anounced on April 10, 2020, and the Decentralized Privacy-Preserving Proximity Tracing protocol (DP3T), proposed by a group of technologists, legal experts, engineers and epidemiologists. It also considers the EU toolbox for the use of mobile applications for contact tracing. [3]

According to the European Commission, contact tracing apps, if fully compliant with EU rules and well-coordinated, can play a key role in all phases of pandemic crisis

[1] Given the rapid development in this field, this is the 1.0 edition, dated 22 April 2020 of a rolling text, which will be updated, if and when deemed necessary.

[2] Beatriz Botero Arcila is a PhD candidate at Harvard Law School, a fellow at the Harvard Berkman Klein Center, and an Advisor to the ICT4Peace Foundation. The author thanks Anne-Marie Buzatu for her inputs and editing of this text, and Daniel Stauffacher, Sanjana Hattotuwa Nele Achten, Serge Droz and Urs Gasser for their review and inputs.

[3] eHealth Network, Mobile applications to support contact tracing in the EU's fight against COVID-10, Version 10. April 15, 2020 https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

management, and are especially helpful when the time is ripe to gradually lift social distancing measures.[4] The toolbox emphasizes that the use of these applications must be voluntary, approved by the national health authority, privacy-preserving and dismantled as soon as no longer needed.[5] Similarly, Google and Apple's initiative emphasize privacy, transparency and consent as of utmost importance in this effort. [6] Both in Europe and in the US there have been other efforts and initiatives along similar lines, and at the time of writing there is an ongoing rift between models that prioritize centralized or decentralized models of data-storage.[7]

Indeed, contact tracing apps touch upon classical cybersecurity and privacy issues in which both governance and design decisions intersect: Who has access to this information and for what purposes? What are the policy goals of the uses of these technologies and who is overseeing these? How are individuals being protected from potentially harmful and/or unintended consequences of the collection of this information? How much access should governments and corporations have to personal information that can be used to address a public-health threat? How are the public ends balanced against the potential risks these applications pose to privacy and other human rights? How will these applications interact with other rights, in this case, the rights to health, mobility, work, education, and privacy?

This document will evaluate the two above mentioned protocols, and what is known about their governance and design at the time of writing. The document should be useful for policy-makers and members of civil society currently looking to evaluate these two different contact-tracing applications as a means to ease the lockdown imposed on most of the world to flatten the curve of infection of Covid-19. Similarly, understanding on how the enjoyment of a variety of human rights interacts vis-à-vis the voluntary adoption of these applications, should offer guidance for policymakers, civil society and developers to decide whether to promote these options, and how these applications should be deployed, and when they should be dismantled.

[4] European Commission, Coronavirus: An EU approach for efficient contact tracing apps to support gradual lifting of confinement measures (Press release) 16 April 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_670.
[5] eHealth Network, Mobile applications to support contact tracing in the EU's fight against COVID-10, Version 10. April 15, 2020 https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.
[6] Apple, Google, "Apple and Google partner on COVID-19 contact tracing technology". April 10, 2020. https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ContactTracing-BluetoothSpecificationv1.1.pdf.
[7] *See e.g.* Safepaths http://safepaths.mit.edu/; see Douglas Bousvine, "Rift opens over European coronavirus contact tracing apps," swissinfo.ch https://www.swissinfo.ch/eng/reuters/rift-opens-over-european-coronavirus-contact-tracing-apps/45703170; "Joint statement on Contact Tracing, April 19, 2020" https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view.

In our analysis, we take a human centric-approach to cybersecurity – considering information breaches or hacking attacks from the perspective of the individual instead of states - and a privacy lens to analyze how the different technical decisions and governance decisions of these applications have different impacts on individual privacy and the exercise of other human rights. We conclude that the two primary models evaluated here are privacy-wise secure, in particular the DT3P protocol. However, their effectiveness will largely depend on their adoption rates and on other broad policy measures that need to be taken by governments to address the pandemic, such as making testing easily available and providing support to individuals who need to self-isolate and may not have the means to do so. Other contact-tracing applications, with different design and governance logics, will most likely create different risks, and so our conclusions should not be extrapolated to those. Our analysis could provide a framework for civil society members and polilcy makers analyzing those models.

The document proceeds as follows: First, it briefly explains contact tracing apps and the main design questions that have been set forth by both the European Commission framework and the Google and Apple partnership. Second, it maps the main risks posed by these applications in terms of data stewardship, network security and the enjoyment of human rights. Third, based on the map of risks developed in section two, we propose a series of considerations that governments should have in mind to (1) adopt urgent institutional mechanisms - such as rules and privacy policies - to mitigate some of the risks posed by these technologies, (2) make design decisions about these applications when applicable, (3) disclose when and how these applications will be dismantled.

## 2. The role of contact tracing applications in combating Covid-19

Contact tracing is a long-used method to address contagious diseases outbreaks and de-escalation of contagion measures. Its main objectives are to allow public health authorities to rapidly identify the individuals with whom a confirmed case of Covid-19 has had contact, ask them to self-quarantine, and rapidly test and isolate/treat them if they have contracted the disease. Contact tracing is normally carried out manually by public health authorities. Since there is no proven treatment currently available for Covid-19, and a vaccine will not be available for several months, the only approaches to stop the epidemic are classic epidemic control measures: identified case isolation, contact tracing and quarantine, and physical distancing and hygiene measures.

According to a study by the Oxford University Big Data Institute, around half of infected individuals become reported cases. When intensive care support is available, the case fatality rate is approximately 2%. About 5% of patients require intensive care support.

Fatality rates are likely to be higher in older populations and in low-income settings where critical care facilities are lacking. Consequently, most efforts geared towards “flattening the curve” of infection aim to avoid overwhelming hospital capacity, while at the same time trying to “buy time” for healthcare facilities to prepare for a larger influx of patients.[8]

Contact tracing and quarantine endeavour to stop the spread of the virus by reducing the number of transmissions from symptomatic individuals and their contacts. In the Covid-19 scenario, manual contact tracing poses a particular challenge because manual contact tracing predominantly relies on the patient's memory, which is less reliable as the period of incubation of the virus is relatively long (up to 14 days) and the virus can be transmitted before symptoms appear.[9] This is especially the case in scenarios in which lock-downs are gradually lifted. Contact tracing and warning applications promise to make that process more efficient, accurate and speedy.[10]

In essence these applications keep a temporary record of proximity events between individuals and alert users of recent contacts with diagnosed cases, prompting them to self-isolate. The Oxford University study suggests that instantaneous communications of contact replaces a week’s work of manual contact tracing work. It also suggests that 60% of a country’s population would need to participate for the approach to be effective.[11] In this sense, the EU Commission document recognizes that a fragmented and uncoordinated approach to contact tracing risks hampering the effectiveness of measures aimed at combating the Covid-19 crisis.

There may be important things being lost with a purely technical contact-tracing approach, however. In Massachusetts, US, the state has rolled out an ambitious manual contact tracing program, hiring 1000 people. The program is built around one-on-one telephone interviews of newly diagnosed patients and their contacts that can last up to an hour. The interviews take an inventory of symptoms, talk the contact through quarantine requirements, and help arrange assistance with food or housing if the contact cannot easily quarantine. The proponents of the program highlight this human contact creates a feeling of confidence and comfort is crucial to encourage collaboration.[12] The downsides are, however, that human-contact tracing is hard to scale because of resource

[8] Luca Ferretti et. al. “Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science, 31 March 2020.
[9] *See:* eHealth Network, Mobile applications to support contact tracing in the EU’s fight against COVID-10, Version 10. April 15, 2020 p. 7.
[10] *See*: “Joint statement on Contact Tracing, April 19, 2020” https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view.
[11] *Id*.
[12] Ellen Barry, An Army of Virus Tracers Takes Shape in Massachusetts, The New York Times, April 16, 2020. Available: https://www.nytimes.com/2020/04/16/us/coronavirus-massachusetts-contact-tracing.html

constraints, it can overlook contacts a subject may not recall or may not know and it is slow.[13]

## 3. Privacy preserving technology

There are three main design decisions that distinguish the privacy and cybersecurity risks contact-tracing applications pose to individuals. First is where and how the data is stored. Second, the technology used to record proximity with other users. Third, the mechanism to report a contact. These design decisions interact with governance decisions such as the kind of access public authorities have to the information recorded, the role they have authorizing and sending messages through the applications. Additionally, they also interact with the socio-economic circumstances of a particular society like access to the Internet and smartphones, to the kind of resources available for individuals who are flagged as contacts and should self-isolate. In this section we map the design features of these applications, and in the following section we map how these applications interact with governance and institutional frameworks.

### *A. Data Storage*

The three main questions regarding data storage: Where is the information stored, how is it stored, and what information is stored. Decentralized solutions - which are favoured in both of the protocols considered here - store data points in each individual's device and centralized solutions store data-points in one server.

In terms of how the information is stored, the log identifiers can be more or less anonymous. Names or phone numbers are not anonymous information, but IDs and randomly generated keys can be. This latter form of identifiers enhances protection against eavesdropping and hacking and doesn't provide information to the public or government to identify individual contacts who may be carriers of the pathogen.

Apple and Google's protocol uses a solution that combines a decentralized architecture with the use of random generated IDs so that users' locations and identities are not shared. The application does not use location for proximity detection. Instead it uses Bluetooth beaconing to detect proximity of users via randomly generated IDs that change

[13] *See;* Marcel Salathé and Ciro Cattutto, "Covid-19 Response: What Data is Needed for Digital Contact Tracing?" DP3T https://github.com/DP-3T/documents/blob/master/COVID19%20Response%20-%20What%20Data%20Is%20Necessary%20For%20Digital%20Proximity%20Tracing.pdf.

every 15 minutes, and it generates a daily tracing key to be correlated to the user.[14] The proximity data related to contacts generated by the app remain only on the device of users and the apps generate arbitrary identifiers (keys) of the phones that are in contact with the user. No user or additional personal information is stored on the device. Similarly, in the case of the DP3T solution, the installed application broadcasted random generated IDs, and stores IDs of phones that have been in proximity.[15]

Finally, the amount of information that is stored has effects on the usefulness of the application. An application that only seeks to identify contacts will only record contact data points; logs that show that two devices were within a few meters and for a few minutes.[16] Such an application will be useful only to identify individuals that have had contact with people who inform the application that they have tested positive and are symptomatic. According to the WHO the main form of transmission is contact with symptomatic people, however, contact with surface or airborne transmission is likely to play a role too. Applications that do not store locational data will, however, be useful to map this kind of contact. They will also not offer less information for epidemiologists to understand the disease.[17]

### *B. Tracking technology*

Regarding the technology used to track proximity, DP3T and Google and Apple's proposal rely on protocols that would support the use of Bluetooth LE (Low Energy) for proximity detection of nearby mobile phones and for the data exchange mechanism.[18] Bluetooth signals could deliver misleading information when it detects proximity in cases where people are wearing masks or are on opposite sides of a wall, and thus they should not be main indicators of whether a person is or isn't infected. In particular, they should

[14] Apple, Google "Contact Tracing: Bluetooth specification V.1.1." April 2020 https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ContactTracing-BluetoothSpecificationv1.1.pdf.
[15] *See*: Carmela Troncoso et.al. Decentralized Privacy Preserving Proximity Tracing p. 3 https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Data%20Protection%20and%20Security.pdf.
[16] *See:* Marcel Salathé and Ciro Cattutto, "Covid-19 Response: What Data is Needed for Digital Contact Tracing?" DP3T https://github.com/DP-3T/documents/blob/master/COVID19%20Response%20-%20What%20Data%20Is%20Necessary%20For%20Digital%20Proximity%20Tracing.pdf; Google, Apple "Apple and Google partner on COVID-19 contact tracing technology", April 10, 2020 https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/
[17] *Id.*
[18] *See:* eHealth Network, Mobile applications to support contact tracing in the EU's fight against COVID-10, Version 1.0. April 15, 2020, p. 10 https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

never replace testing. Notwithstanding, bluetooth tracking is more accurate and privacy preserving than GPS and cell site information, as there is no need to log location.[19]

This is how Bluetooth signals work: When two users of the app come near each other, both apps estimate the distance between each other using Bluetooth signal strength. If the apps estimate that they are less than approximately six feet (or two meters) apart for a sufficient period of time, the apps exchange identifiers. Each app logs an encounter with the other's identifier. The users' location is not necessary, as the application need only know if the users are sufficiently close together to create a risk of infection.

### *C. Reporting*

Reporting happens when a user tests positive and this information is communicated to those with whom they have been in contact. In a decentralized model like the ones discussed here a user uploads its identifiers from their phone to a backend server. From this data, the identity of the patient cannot be easily derived by the server or by the apps of other users. Each app constantly reviews the backend to locally compute whether the app's user was in physical proximity of an infected person and potentially at risk of infection. If they were, the app then informs the user to take action.[20]

The design decisions regarding how reporting is handled can have an impact on the role public authorities play. The European Union document suggests that in decentralized applications health authorities should approve when a user notifies the app that they have tested positive.[21] An advantage of this kind semi-decentralized reporting mechanism is that the report is certified by an authority. Similarly, in the DP3T protocol, the reporting signal for a patient that has been diagnosed with the virus is only sent with their consent and with authorization from a health authority.[22] Other models, not examined here, have suggested that more information be collected to give a party operating the server access to locational data of a contacted individual, for example, which could give authorities acceess to potential epicenters of contagion.[23]

[19] Andrew Crocker et.al "The Challenge of Proximity Apps for Covid-19 Contact Tracing" EFF April 10, 2020 https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing.
[20] Carmela Troncoso et.al. Decentralized Privacy Preserving Proximity Tracing p. 3 https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Data%20Protection%20and%20Security.pdf.
[21] eHealth Network, Mobile applications to support contact tracing in the EU's fight against COVID-19, Version 10. April 15, 2020, p. 15 https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf
[22] Carmela Troncoso et.al. Decentralized Privacy Preserving Proximity Tracing p. 3 https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Data%20Protection%20and%20Security.pdf
[23] *See* "Rift opens over European coronavirus contact tracing apps," swissinfo.chhttps://www.swissinfo.ch/eng/reuters/rift-opens-over-european-coronavirus-contact-tracing-apps/45703170;

This approach, however, seems to be at odds with the principles of the protocols examined here: In the UK, the NHS expressed its intention to have access to the information of people who tested positive, which would have allowed it to access general populations flows in the aggregate or information about people who opted in. Google and Apple, however, refused to support the NHS in this effort.[24]

### 4. Risks and governance considerations

As explained in the introduction, our analysis focuses on network security, data-stewardship and the protection of human rights. Contact-tracing applications pose direct risks to individual privacy and self-determination, many of which are addressed by the decentralized architectures of the protocols reviewed here. Lockdowns, however, are also having tremendous socio-economic effects as unemployment increases, businesses of all sizes are at risk of bankruptcy, and the effects of lockdown will already have long lasting effects on children, youth and young adults whose education or career development paths have been affected. Furthermore, these socio-economic effects carry the potential to reinforce existing inequality patterns and risks for their future livelihood.[25] In this section we map some of the main ways in which contact-tracing interacts with human rights and point out some of the effectiveness considerations policy-makers and other actors should take into account when considering adopting these applications.

## B. Network safety and governance challenges

As all digital technologies, contact-tracing applications pose privacy-related risks to its users. In particular, it is a general concern that third parties who can access the information collected can use it for other unintended purposes The two protocols considered here, however, mitigate most of these risks by storing data in non-identifiable ways in individual phones.

The applications, however, are still vulnerable to attacks or back-end impersonation. These attacks can affect the trustworthiness of information in the contact-tracing apps networks and the trustworthiness of their systems of alerts. Both DP3T and the Apple and

[24] Alex Hern, “NHS in standoff with Apple and Google over coronavirus tracing” The Guardian, April 16, 2020.

[25] Covid-19 Rapid Response Initiative, Whie Paper 5. Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 while Mitigating Privacy Risks, April 3, 2020; Annie Lowrey, Millenials Don’t Stand a Chance, The Atlantic, April 13, 2020 https://www.theatlantic.com/ideas/archive/2020/04/millennials-are-new-lost-generation/609832/; The World Bank, The Economy in the Time of Covid 19, April 2020 https://openknowledge.worldbank.org/bitstream/handle/10986/33555/9781464815706.pdf?sequence=5

Google protocol proposed decentralized systems to limit these risks by collecting the minimum amount of information, protecting non-infected users, and including data-deletion and dismantling plans.

(1) *Data minimization:* Both protocols analyzed here foresee collecting the minimum amount of information possible and store it in the form of the logs described before on each device and on the backend server. Consequently, no entity can use or abuse the information for any other ends. However, it comes at the cost that no entity keeps records of a social group or gain aggregated information about the spread of the disease.
(2) *Protecting non-infected users*. No entity, including the backend server, can learn information from non-infected users.
(3) *Graceful dismantling*. Both the Apple and Google Protocol and the DP3T pandemic mention that the system will organically dismantle itself after the end of the epidemic. Infected patients will stop uploading their data to the central server, and people will stop using the app. The DP3T protocol includes that data on the server is removed after 14 days.[26]

The systems architecture, however, remains vulnerable to the following challenges:

*Network attacks and reidentification*

(1) A tech-savvy user could reidentify an infected user's IDs with whom they have been physically close to in the past by modifying the app on their device and collecting extra information about other users. When an ID is broadcasted as belonging to an infected user, the tech-savvy user could thus re-identify the infected user. The DP3T documentation clarifies that this risk is inherent to any proximity-based system notification system.[27]
(2) (2) A tech-savvy user deploying an antenna to eavesdrop on bluetooth connections can learn which connections correspond to infected people, and then can estimate the percentage of infected people in a small radius of 50m. If in addition, the user has a camera, he can capture images and potentially re-identify those people.[28]

For non-tech savvy adversaries, the type of "anonymous" identifiers proposed by Apple and Google and by DP3T protocol will preserve the anonymity of the users participating

[26] *See*:Carmela Troncoso et.al. Decentralized Privacy Preserving Proximity Tracing p. 3 https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Data%20Protection%20and%20Security.pdf
[27] *Id.*
[28] *Id.*

in the network. It will be important that these are randomly assigned as an adversary could learn that multiple identifiers belong to the same infected user increasing the risk that they can tie that activity to a real person.[29]

To additionally lower the risks associated with possible network attacks, developers should open-source their code and subject it to third-party audits and penetration testing.[30] They should also publish details about their security practices.[31]

*Trolling*

Trolling is a risk that is hardly mitigated in purely voluntary systems, as ill-intentioned individuals could send false alerts. The EU documents and the DP3T protocol mitigate this risk by suggesting that health authorities should approve when a user notifies the network that they have tested positive. The Google and Apple protocol remains vulnerable to this risk.

*Additional privacy controls*

Though in both the protocols analyzed here no third party will have access to personal information it is worth remarking that the European Data Protection Board recently clarified how the EU General Data Protection Regulation (GDPR) and other data protection laws apply to the current situation. According to the Statement, if public authorities obtain personal information for the purposes of the pandemic, it should be processed for specified and explicit purposes, individuals must receive transparent information on the processing activities that are being carried out, and security measures and confidentiality policies must be adopted to prevent disclosure of personal data to unauthorised parties. The Statement clarifies that the GDPR allows competent public authorities to process personal data in the context of an epidemic, in the context of national laws and the conditions set therein. Under those circumstances individual consent is not needed.[32]

[29] *Id.*
[30] Serge Vaudenay, "Analysis of DP3T Between Scylla and Charybdis," April 8, 2020 https://eprint.iacr.org/2020/399.pdf
[31] ANDREW CROCKER, KURT OPSAHL, AND BENNETT CYPHERS, The Challenge of Proximity Apps For COVID-19 Contact Tracing - APRIL 10, 2020 https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing
[32] European Data Protection Board, "Statement on the processing of personal data in the context of the COVID-19 outbreak. Adopted on 19 March 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

In both the US and Europe, however, those who have access and can use consumer data will largely be determined by the privacy policies of the entities collecting data. In the case of contact-tracing apps, this will be the entity operating the back-end. To the extent Google and Apple are main market players with significant leverage over developers that use their APIs to develop individual apps, they could include in the terms of service that govern the use of their APIs provisions that enhance user privacy as an additional safety-mechanism.

In both the protocols analyzed here, many of these measures are in place already. However, to the extent governments develop their own contact-tracing applications, and access information from infected individuals or decide to include into their contact tracing efforts data from other sources - including public transport ticketing and credit-card records, as it was done in Korea and Taiwan[33] _ enforceable privacy-enhancing rules and policies governing should be included in these applications.

The following privacy policies to be included are recommended:[34]

1. **Deletion and Data Minimization**: As little information as is needed should be collected. Back-end operators should have no access to any personal information, and collected information should be automatically deleted once it is no longer needed, meaning that information should only be stored during the incubation time of the virus, about 2 weeks.

2. **Restricted use:** The information collected and/or shared to with trusted authorities should only be used for reasons directly related to addressing the public health crisis. It must be explicitly kept out of reach of criminal law enforcement authorities, intelligence agencies, and immigration authorities. Furthermore, the commercialization of this information must be forbidden.

3. **Transparency:** Individuals must at all times have a means to know, easily and in a clear manner, how their information is being used when governments or other trusted authorities have had access to it (i.e. because they have authorized a message signaling potential contagion).

[33] Ross Anderson, Contact Tracing in the Real World https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world/?utm_campaign=The%20Interface&utm_medium=email&utm_source=Revue%20newsletter

[34] For a similar set of suggestions see ACLU, "Apple and Google Announced a Coronavirus Tracking System. How Worried Should We Be?" April 16, 2020 https://www.aclu.org/news/privacy-technology/apple-and-google-announced-a-coronavirus-tracking-system-how-worried-should-we-be/

4. **Consent:** Whenever possible, a person testing positive must consent to any data sharing by the app. The decision to use a tracking app should be voluntary and uncoerced. Installation, use, or reporting must not be a precondition for returning to work or school, for example.

5. **Roll-out strategies:** Publicly and privately sponsored strategies must include from the beginning parameters regarding when an application will be discontinued in different places as well as when it is closed down completely. This could be, for example, when the WHO declares that the pandemic is over, when certain areas are declared Covid-19 free, when universal testing is made available or when a vaccine is developed. At the moment, exactly what this threshold is is absent both in the Apple and Google and the DP3T protocols.

6. **Anti-discrimination and voluntariness:** Vulnerable groups are often disparately burdened by surveillance technology. They are also often "frontline workers" who are the most exposed. They may also often lack access to the Internet or smartphones. Participating in contact-tracing networks like the ones analyzed here should never be required to enjoy other fundamental rights, such as the right to work, education or participating in a social program. An exception could be made if those programs or activities provide a viable and dignified alternative (such as work from home, education from home, and paid sick-or quarantine leave). For the same reason, governments should also never condition the enjoyment of a fundamental right to opt-ing in to any of these applications.[35]

## C. Governance challenges in contexts of high inequality

Contact tracing applications assume widespread access to smartphones, an internet connection and a reasonable place for people to self-isolate. To be effective, they also require widespread and accessible testing. These features may not correspond to the reality of many countries in the global south or, in the global north, the realities of many minority/vulnerable communities.

[35] Andrew Crocker, et. al., The Challenge of Proximity Apps For COVID-19 Contact Tracing - April 10, 2020 https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing

*Contact tracing and inequality*

Decision-making based on data driven applications can distort realities, as access is not uniform. This can have dangerous consequences for both public health and human rights if no corrective measures are set in place. According to a white paper by the Saffra Center at Harvard University, more than 70% of the population would install contact-tracing applications for optimal performance, although lower penetration could also be combined with other contact tracing interventions. One study estimates that 40% of adoption would be the minimum, while another indicates 60 to 80% would be the minimum penetration required. These are high thresholds. Governments and policy-makers will have to consider the likely percentage of voluntary participation in contact tracing schemes to estimate their effectiveness.

Additionally, those who do not install contact tracing applications may be populations at higher risk of contagion. In the US context, the most vulnerable populations - who share characteristics such as race, income, age and occupation - are disproportionately exposed and have higher mortality rates. These same populations would also not be able to participate in contact tracing in the same percentages as other members of the population as they also have significantly less access to smartphones and Internet connectivity. The same is true in most countries in the global south where Internet and smartphone adoption is below the 60% threshold.[36] Low levels of adoption will affect their overall effectiveness, though they may not be harmful for individuals adopting them. In such scenarios, however, it is important that users are aware that these applications provide limited information about their possible contacts.

Lastly, voluntary contact-tracing and voluntary self-isolation assumes that people have the means and space to self-isolate. In many countries, however, many households live from hand to mouth and they do not have the resources to cope with self-isolation. If individuals don't have access to sick-leave or no "self-isolation" insurance or aid, the decision to self-isolate may be one that risks the means to feed themselves and their families.[37]

[36] *See* Helani Galpaya, et. al. "After Access: ICT and use in Sri Lanka and the Global South" (Report) 22 May, 2019.
[37] *See e.g.* World Bank, The Economy in the Time of Covid 19, April 2020 https://openknowledge.worldbank.org/bitstream/handle/10986/33555/9781464815706.pdf?sequence=5

Self-isolation may also be impossible for people living in slums or in crowded housing, for homeless people, migrant workers and those without access to clean water or sanitation facilities.[38]

*Contact-tracing and discrimination*

Though the protocols considered here are voluntary, and in the case of Apple and Google's app not even the back-end receives information on infected individuals, it is not unlikely that, as they are deployed, workplaces and educational institutions will require their employees and students to download these apps. Similarly, it is not unlikely that these or other apps evolve into "safety passes" showing third parties that the owner of the cellphone has not been in close contact with an infected person and/or is not a carrier.[39] In these contexts, contact-tracing apps risk increasing discrimination to individuals who decide not adopt an application or don't have the means to.

In scenarios in which governments access some form of information collected by applications - for example on who has tested positive or their geolocation - governments must be wary not to over-rely on this information, as the most vulnerable populations may not appear on the data for lack of access and lack of trust in the system. Paradoxically, this kind of policy-blindness will leave unprotected those who need protection the most.

## D. Governance and enhancing trust

One of the reasons why the state of Massachusetts decided to adopt a human-contact tracing program was because "the bond of trust formed by a human contact trace."[40] It is not impossible that contact-tracing applications are also effective in helping different communities locate potentially infected people, asking them to self-isolate, and testing them and quarantining them. This can only be done, however, when the applications are released in line with policy responses that enhance individual trust not only in the applications but in the public policies and institutional setting put in place to address the pandemic: Trust that they will not lose their jobs or income if they self-isolate, trust that

[38] *Id. see also* Cahy O'Neal The Covid-19 Tracking App Won't Work Bloomberg, April 15, 2020. https://www.msn.com/en-sg/news/techandscience/the-covid-19-tracking-app-won-e2-80-99t-work/ar-BB12GXU0

[39] For an idea about how such a safety pass could work see Daniel Goodwin "Architecting the BioCensus" Medium Collection, April 17 2020. https://medium.com/@danielrgoodwin/architecting-the-biocensus-9da1d3399359

[40] Ellen Barry, An Army of Virus Tracers Takes Shape in Massachusetts, The New York Times, April 16, 2020. Available: https://www.nytimes.com/2020/04/16/us/coronavirus-massachusetts-contact-tracing.html

there will be institutions in place that will assist them with food or housing if they need it, and that they will not be penalized if they don't adopt the applications.

When the adoption of the application is voluntary, as is the case in the two protocols reviewed here, enhancing trust in these applications and the institutions in place to address the pandemic will be crucial to guarantee that they are widely adopted when possible and that people decide to self-isolate when so needed.

Relatedly, governments that want to promote these applications as part of their economic and social measures may decide to subsidize access to the Internet and smartphones.[41]

Finally, enhancing trust in the systems in which these applications are deployed will depend too on making healthcare more accessible, enhancing the capacity of existing healthcare systems, and enabling wide-spread testing. As is the case in Massachusetts, opt-in schemes in which individuals can choose to receive a phone call from mental health caregivers or human contact-tracers, who can then walk them through the process of self-isolation, can also improve the whole trustworthiness of the system. If individuals know there is a system that is supportive of their needs, they may be more likely to collaborate with it.

## 5. Evaluating the effectiveness of contact-tracing applications

Application-enabled contact tracing can be an effective means to enable disease decline and avoid multiple peak periods and disease resurgence.[42] Voluntary contact-tracing is also a tool that can better inform individuals about their risks, solicit testing, and take measures, which can in turn help governments have a more targeted approach to attend to those most likely to have been exposed, so that the pathogen can be isolated.[43] In order to be successful, these applications will need (1) to be widely adopted, (2) that there are institutional measures in place that make self-isolation possible and (3) that testing is easily available. This last measure is important to identify infected individuals and inform the system, but also to inform those who are not infected that they can leave self-isolation.

[41] See for example Internet subsidies in Colombia: Ministerio de Tecnologías de la Información, "Esquema de subsidios para Internet en estratos 1 y 2" https://www.mintic.gov.co/portal/inicio/Iniciativas/Servicios/Esquema-de-subsidios-para-internet-en-estratos-1-y-2/.

[42] Ramesh Raskar, Apps Gone Rogue - Safepaths https://arxiv.org/pdf/2003.08567.pdf

[43] *See* Covid-19 Rapid Response Initiative, Whie Paper 5. Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 while Mitigating Privacy Risks, April 3, 2020 p. 5

Finally, (4) it is likely that these applications will compliment, but not replace, government efforts to implement institutional contact tracing as in the state of Massachusetts.

Especially when their adoption is voluntary, contact tracing applications will only be effective if individuals are able to trust them, including that use of the application and any consequences that flow therefrom such as the need to self-isolate will not create additional risks to their livelihoods.

In the two models we have reviewed in this document, we have found no significant risks related to user privacy, or the fact that government institutions or third parties can collect personal information, that can be later used for other means. This is achieved mainly because (1) they collect the least amount of information possible, and in an almost anonymous way, (2) they store all information in individual devices and share minimal information with third parties and the network.

As a joint statement of computer scientists from all over the world points out, models that enable a form of government or private sector surveillance could significantly undermine trust in and acceptance of these applications by society at large. In post-pandemic times, it is vital that these applications are removed and do not enable further surveillance in our societies. Thus, solutions which would allow for invasions of privacy through reconstruction of information about the population should be rejected without further discussion.[44]

The main risks the Apple and Google and DT3P protocols pose are that (1) if they are not widely adopted they generate a false sense of safety, (2) they feed into patterns of inequality and discrimination, creating mis-trust between app users and non-app users and (3) they burden the weakest of society with requirements to self-isolate when it is extremely costly for them to do so, and (4) they mention the applications will be rolled-out when the pandemic is over, but do not establish exactly by whom or how will this be determined.

To address these risks, and realize the promise of these applications, governments should thus not consider these technologies as alternatives to much needed policy-packages that seek to expand the capacity of health systems and facilities, enhance access to healthcare, expand testing, and create a safety net for those in need.[45] Lastly,

[44] "Joint statement on Contact Tracing, April 19, 2020" https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view

[45] *See* Petral Molnar and Diego Naranjo, "Surveillance Won't Stop the Coronavirus", The New York Times, April 15, 2020

entities operating these applications should be transparent about the architectural and governance decisions governing these applications.[46]

Furthermore, where governments use contact-tracing apps to gain aggregated data or locational data of positive cases, they should always bear in mind that digital technologies are unevenly adopted, often not including the most vulnerable in a society, and their decision-making processes should be informed accordingly.

## Conclusion

A fundamental rights perspective and a human centric-approach to cybersecurity allows policy-makers and civil society to identify the different ways in which contact-tracing apps interact with other measures to address the effects of the Covid-19 pandemics and affect the enjoyment of different fundamental rights.

In this document, we have reviewed the DP3T and Google and Apple protocols, the two main ones at the time of writing. We have identified the main risks contact-tracing applications pose, how they address them and suggested the accompanying measures that should be implemented when these applications are rolled out. Such accompanying measures will be crucial both to enhance their safety, but also trust in them and their effectiveness.

Contact-tracing applications could be effective as a means to help contain the pandemic when the time is right to ease some lockdown measures, and to contain subsequent outbreaks. Their deployment should also help governments slowly re-open local economies and be more effective at directing other efforts - like health-care attention or testing - to those who might be at higher risk. It is of the utmost importance, however, that as these applications - with the safeguards we have considered and reviewed here - are rolled out, that they are accompanied by measures that make testing accessible and build safety nets for vulnerable and underserved populations who are at higher risk. They will not, however, replace them.

ICT4Peace Foundation, Geneva, 22 April 2020

[46] “Testing and public health response—in programs established by states and administered by local health authorities—can and should be fully aligned with civil liberties, due process, non-discrimination, data and health privacy protections, and health ethics.” Danielle Allen et. al. “Roadmap to Pandemic Resilience” EDMOND J. SAFRA CENTER FOR ETHICS AT HARVARD UNIVERSITY, April 20, 2020 https://ethics.harvard.edu/files/center-for-ethics/files/roadmaptopandemicresilience_final_0.pdf