Digital contact tracing against COVID-19: a governance framework to build trust

Sacha Alanoca*, Nicolas Guetta-Jeanrenaud**, Isabela Ferrari***, Nyasha Weinberg****, R. Buse Çetin***** and Nicolas Miailhe******

Global context
An unprecedented health crisis, raising complex social, economical, and ethical trade-offs

Since the outbreak of COVID-19 in late 2019 and its classification as a pandemic by the World Health Organization (WHO) in March 2020, the numbers of deaths and infections have continued to rise globally. As of December 2020, the count is at over 70 million diagnosed cases and over 1.5 million deaths.1 In Latin America, numbers have spiked recently, reaching over 14 million infections and 470,000 deaths, with the highest number of cases respectively in Brazil, Argentina, and Colombia.2 According to the WHO, the transmission rate (R0) of COVID-19 in Wuhan in January and February—prior to the implementation of comprehensive control measures—was 2–2.5,3 making COVID-19 highly contagious.4 Facing this unprecedented crisis, most
Contact Tracing as an effective mitigation technique

Confronted with the urgent need to mitigate the crisis, governments around the world have explored a combination of health care and technological tools. ‘Contact tracing’ describes a variety of techniques used to identify people who may have come into contact with a positively diagnosed individual, and take appropriate action to inform, isolate, and treat those contacts.

The current debate over ‘digital’ contact tracing tends to overshadow the fact that ‘manual’ contact tracing has systematically been deployed in the past to mitigate epidemics such as tuberculosis, measles, HIV and, more recently, to limit the spread of Ebola and SARS. Relative to other diseases of the similar type, COVID-19 is considered to be highly contagious: it has a median incubation period of five days, with 97.5 per cent of those who develop symptoms doing so within 11.5 days. Estimates of the asymptomatic share of infected individuals range from 15.5 per cent to 56 per cent. In this context, labour-intensive manual contact tracing, which relies on human memory and trained medical staff, lacks both speed and accuracy to match the spread of the virus.

Digital contact tracing can ‘improve’ manual contact tracing through the mobilization of digital planning and analytics, and ‘automate’ the process via a smartphone or smart bracelet for proximity tracking or digital health monitoring. By facilitating targeted testing of ‘at-risk’ individuals, digital contact tracing helps to break contamination chains. When coupled with appropriate measures such as social distancing, testing, and self-quarantine, it could be a key component to an effective strategy to contain the spread of COVID-19. Several countries which have managed to ‘flatten the curve’ of the first wave—such as Taiwan, South Korea, or Singapore—have deployed digital contact tracing as part of their strategy. According to the COVID-19 Digital Rights Tracker, there are currently 120 contact tracing applications deployed across 71 countries (Figure 1).

However, worldwide concerns have been raised over the widespread and generalized adoption of digital contact tracing applications. Issues include their purpose, performance, impacts on privacy, data protection, human agency, and risks of stigmatization. Many of these emanate from mistrust in public authorities or technology firms, and fear of establishing mass surveillance. Disinformation and the lack of clear ethical, legal, and technical safeguards have polarized the public debate at a time when we need to build trust, and should not have to sacrifice civil liberties for public health. There is therefore a pressing need to co-design governance mechanisms that capture the health benefits of contact tracing applications while mitigating their potential risks and adverse effects. The urgency of the situation should not
impact our collective ability to make informed decisions, and to responsibly navigate potential tensions between public health, safety and civil liberties. Evidence suggests that the widespread adoption and efficacy of contact tracing applications is reliant on public trust and social acceptability, further reinforcing the need for ethical and legal frameworks governing their development.

This article aims to shed light on problems related to digital contact tracing. Therefore, considering: (i) that this is an unprecedented global situation; (ii) that the operation of these tools is still largely misunderstood, especially by legal experts; and (iii) that this knowledge is essential to evaluate their potential to assist in health crises, to understand the real dimension of their risks and, therefore, to regulate them; one considers that addressing the theme could not be done without a detailed overview on contact tracing methods and technical features.

Technical alternatives and tradeoffs

Contact tracing applications can be based on a range of technologies and privacy-preserving protocols (see Figure 2). They can be voluntary—available for consenting individuals on mobile application stores—mandatory, or nudged. The data collection process can be proximity-based (usually acquired through Bluetooth), rely on GPS localization data, or both. Data can be stored locally on the individuals’ mobile devices in a decentralized approach, on a centralized server, or with a mixed approach. Finally, the analysis that is conducted by the relevant authority can range from simple proximity calculation to epidemiological modelling, hotspot mapping, and more.

Application installation

A technical imperative to the success of a contact tracing application is widespread installation. Once the application is downloaded, the contact tracing feature operates in the background of the device. While there is still no consensus among epidemiologists on the modelling assumptions of COVID-19 transmission—which depend on the number of cases, the R0 transmission rate, social customs, broader health strategies, and more—one initial study estimated that a contact tracing application with a minimum adoption rate of 60 per cent could effectively ‘stop the epidemic’. However, this is an upper bound, and the authors of the report subsequently pointed out that lower levels of adoption could be vital to curbing the spread of the virus.17

Figure 1: The ‘Perú en tus manos’ application by the Peruvian Government.

16 ‘Digital Contact Tracing Can Slow or Even Stop Coronavirus Transmission and Ease Us out of Lockdown’ (University of Oxford Research) <https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown/> accessed 3 July 2020.

17 ‘No, Coronavirus Apps Don’t Need 60% Adoption to Be Effective’ MIT Technology Review <https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/> accessed 3 July 2020.
Installation of the application is a sizable issue for governments fighting COVID-19. Several countries have taken the radical approach of making the application mandatory for all citizens. China’s ‘contact detector’ plugs into the existing and widely used applications WeChat and Alipay. The programme analyses health and travel data to assign ‘risk colors’ to individuals, potentially denying them access to stores and essential services.\(^\text{18}\) In other countries, such as Kuwait or Bahrain, the application is separate from existing phone functionalities but its installation is mandatory and legally enforced. The vast majority of countries have settled on voluntary applications, although personalized or generic incentives, or ‘nudges’, can be embedded in the application’s functionalities.\(^\text{19}\) Some offer additional advice on where to get tested (Australia) or hospital availability (Turkey), while others release news updates connected to the pandemic (Bulgaria) or health tips (Qatar). The extent to which these additional incentives compel adoption of the application will depend on whether there are alternative routes to access identical services.

**Data collection**

Of the existing contact tracing applications, 25 per cent use GPS, 48 per cent Bluetooth and 22 per cent a combination of both\(^\text{20}\): a distribution which highlights the lack of consensus around the most effective approach.

Bluetooth protocols rely solely on proximity detection. A mobile device records other Bluetooth signals within a given range for a given time: this is known as a ‘digital handshake’. During the exchange, each device collects pseudonymized tokens—typically chains of numbers which change randomly several times a day—as identifiers of the other users. These encrypted tokens can either be stored on local devices or a central server (see Data Storage section); regardless, a notification mechanism exists to inform individuals when they have been in proximity of a user signalled as infected.

---

\(^{18}\) Raymond Zhong, ‘China’s Virus Apps May Outlast the Outbreak, Stirring Privacy Fears’ *The New York Times* (26 May 2020) <https://www.nytimes.com/2020/05/26/technology/china-coronavirus-surveillance.html> accessed 24 June 2020.

\(^{19}\) ‘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/> accessed 22 June 2020.

\(^{20}\) Woodhams (n 15).
Countries such as Mexico, Italy, Japan, and the UK have all adopted peer-to-peer Bluetooth Low Energy (BLE) protocols. Singapore also uses the Bluetooth-based BlueTrace protocol. In most cases, proximity is measured as within 1 meter, and pseudonymized tokens are exchanged after 15 minutes (see Figure 3).

On the other hand, GPS schemes rely on mobile data to reconstruct users’ location histories. When individuals are flagged as infected, the contact tracing application retraces every other user with whom they have crossed paths. The GPS protocol offers the additional feature, unavailable with Bluetooth, of identifying geographic hotspots of the virus, thus monitoring local clusters and enabling targeted response. However, this technique is less accurate at recording proximity, especially indoors or during underground travel. GPS protocols have been associated with some of the more privacy-intrusive applications, such as Bahrain’s BeAware, Shlonik in Kuwait, or Norway’s initial application Smittestopp.21

Finally, some application protocols combine Bluetooth and GPS data for contact tracing. The MIT-based Private Kit SafePaths platform uses both GPS and Bluetooth data to record individuals’ locations.22 The protocol is free, open-source, and has been adopted in several countries including Cyprus.23

Data storage

At a minimum, contact tracing applications collect location (GPS) or proximity (Bluetooth) data. France’s StopCovid, for example, has no identification requirements. However, many other applications also request additional personal user information. Ketju in Finland and Hayat Eve Siğar in Turkey, among others, require valid phone numbers for authentication. In other countries, such as Iceland (only for individuals who have been diagnosed with COVID-19), Qatar, and Kuwait, authentication is done using National ID numbers. Some applications, such as ViruSafe in Bulgaria, collect users’ age and medical history at registration. All contact tracing applications also collect COVID-19 diagnosis data to notify at-risk individuals.

Given the sensitive nature of the data at hand, data storage architecture has been consistently and hotly debated among application developers and privacy

21 ‘Bahrain, Kuwait and Norway Contact Tracing Apps a Danger for Privacy’ (Amnesty International) <https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/> accessed 30 June 2020.
22 Andrew Westrope, ‘MIT, Apple, Google Build Apps to Trace COVID-19 Contact’ (Government Technology) <https://www.govtech.com/health/MIT-Apple-Google-Build-Apps-to-Trace-COVID-19-Contact.html> accessed 9 July 2020.
23 ‘Technology Recruited in Fight against Coronavirus’ (Financial Mirror, 6 April 2020) <https://www.financialmirror.com/2020/04/06/technology-recruited-in-fight-against-coronavirus/> accessed 4 July 2020.
experts. In centralized architectures, data collected by contact tracing applications is directly recorded on a main server: this is usually highly secure and accessible for government agencies. Decentralized architectures, on the other hand, keep logs of proximity and location locally on users’ devices. A leading decentralized solution known as Decentralized Privacy-Preserving Proximity Tracing (DP-3T) and developed by a Swiss consortium is featured in several national applications, including that of Finland, Malaysia, and Switzerland. Some European countries—including France’s StopCovid—have also adopted what they call a “centralized-decentralized contact-tracing protocol” (25). The Robust and Privacy-Preserving Proximity Tracing (ROBERT) protocol—a contribution to the Pan European Privacy-Preserving Proximity Tracing initiative (PEPP-PT)—initially stores data on devices but sends pseudonyms of all at-risk users to a centralized server once an individual has tested positive. (26)

The technical debate over data storage protocols provides the backdrop for a political tug-of-war between large technology firms, governments, and supranational bodies. National interests push governments to prefer home-grown solutions: Norway and Columbia for example opted for state-backed designs. In order for applications to be interoperable across country lines, however, technologies must be coordinated and supranational bodies such as the European Union (EU) have argued for a single protocol. Technology firms, leveraging their control over user devices have taken position as well: adoption of DP-3T was accelerated by the fact that Apple and Google’s joint protocol relies on that technology. Apple’s decision to render other protocols interoperable on iPhone—by not allowing background Bluetooth collection—has further crippled the competition. This has convinced countries such as Germany, who initially adopted the ROBERT protocol, to switch over to DP-3T. (29) Today, over a third of contact tracing apps are using Google and Apple’s API. (30)

Most contact tracing applications address privacy concerns by de-identifying data, regardless of whichever storage protocol is selected. Although complete data anonymization is never achievable in practice, different methods of data pseudonymization are integral aspects of most contact tracing applications. Applications such as StopCorona in Austria, StopCovid in France, or TraceTogether in Singapore assign unique IDs to users, which in some cases randomly change over time for additional security. Both the MIT Private Kit SafePath and the Google–Apple protocols use differential privacy to ensure that aggregate data made available by the application does not enable individual users to be re-identified.

Since contact tracing information is only relevant within a given number of days of a person’s diagnosis, most contact tracing applications limit the time period for data storage, after which it is destroyed. Here, findings from the medical world inform application design features: although the typical incubation period of the virus has been evaluated at about 5 days, 14 days has consistently been used in quarantine guidelines. Iceland, Poland, and Tunisia have all developed applications that store user data for no more than two weeks. In Malaysia, decentralized data is kept on the mobile device for 21 days. In Qatar, data is only deleted after 2 months. Some countries such as China, South Korea, and Singapore have not specified how long their applications intend to hold user data.

Data analysis

The data collected by contact tracing applications can serve different purposes for governing authorities. The minimal use of contact tracing data consists in flagging proximity between infected individuals and application users (as measured by Bluetooth or GPS). However, several countries leverage data from contact tracing applications for different purposes. The UK’s initial plan for digital contact tracing saw data collected from the NHS

24 ‘A Flood of Coronavirus Apps Are Tracking Us,’ (n 19).
25 ‘France’s Inria and Germany’s Fraunhofer Detail Their ROBERT Contact-Tracing Protocol’ (TechCrunch) <https://social.techcrunch.com/2020/04/20/frances-inria-and-germanys-fraunhofer-detail-their-rob-ert-contact-tracing-protocol/> accessed 9 July 2020.
26 Claude Castelluccia and others, ‘ROBERT: ROBust and Privacy-Preserving Proximity Tracing’ [2020] HAL-Inria <https://hal.inria.fr/hal-02611265/> accessed 29 July 2020.
27 Javier Espinoza, Joe Miller and Leila Abboud, ‘How Europe Splintered over Contact Tracing Apps’ Financial Times (10 May 2020) <https://www.ft.com/content/7416269b-0477-4a29-815d-7e4ee8100c10> accessed 28 July 2020.
28 Julien Cadot, ‘StopCovid vs Apple: pourquoi la France s’est mise dans une impasse’ (Numaroma, 21 April 2020) <https://www.numaroma.com/tech/619446-stopcovid-vs-apple-pourquoi-la-france-sest-mise-dans-une-impasse.html> accessed 29 July 2020.
29 ‘Germany Flips to Apple-Google Approach on Smartphone Contact Tracing’ Reuters (26 April 2020) <https://www.reuters.com/article/us-health-coronavirus-europe-tech-idUSKCN22807J> accessed 28 July 2020.
30 Woodhams (n 15).
31 Luc Rocher, Julien M Hendrickx and Yves-Alexandre de Montjoye, ‘Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models’ (2019) 10 Nature Communications 3069.
32 Differential privacy is a technique for sharing confidential information about a dataset while preserving privacy: it provides patterns of groups, but withhold information about individuals.
33 Lauer and others (n 11); ‘The Science Behind A 14-Day Quarantine After Possible COVID-19 Exposure’ (NPR.org) <https://www.npr.org/sections/health-shots/2020/04/01/824903684/the-science-behind-a-14-day-quarantine-after-possible-covid-19-exposure> accessed 10 July 2020.
COVID-19 application also feed into epidemiological models to study virus spread.34

Ethical risks raised by digital contact tracing

The adoption of digital contact tracing applications raises serious ethical questions. Given the extent and sensitive nature of the data collected, these technologies have the potential to undermine fundamental civil liberties and human values such as privacy, data protection, human autonomy, and fairness.

Privacy and data protection

All digital contact tracing requires some degree of access to information that could potentially infringe on privacy. This includes health status, location, contacts, and, in some cases, other personal data such as banking or social media information. According to the COVID-19 Digital Rights Tracker, 19 contact tracing applications, totaling 4 million downloads combined, do not have a privacy policy.35 Lack of information and legal, technical, and political safeguards therefore raise major concerns. There are two important aspects of privacy in this context: the ‘actual’ privacy preserving characteristics of the application itself, and the extent to which it offers users ‘control’ over privacy settings. Actual privacy implies limiting information exposure to the greatest extent possible while control over actual privacy means allowing individuals to make transparent choices about the use of their data.36 Fighting against the pandemic through digital contact tracing may require temporary curtailments of actual privacy. Since it potentially raises limitations to privacy, individuals should be empowered to carry out these choices themselves to build trust in and buy-in for the technology adoption.

There is currently much debate among digital privacy experts over the best privacy-preserving application setup (see Figure 4). Bluetooth protocols have privacy advantages over GPS because cryptographically secured contact tokens are much less vulnerable to de-anonymization techniques. However, these protocols are more at risk of trolling because there is no verification of user identity, and people can fake being contagious.37 Malicious individuals could ‘use the app to run service-denial attacks and spread the panic; and little Johnny [can] self-report symptoms to get the whole school sent home’.38

One important aspect of privacy is data pseudonymization. Technical steps taken in this direction by contact tracing applications may not fully mitigate the risk. Several applications, including France’s StopCovid, have been accused of failing to sufficiently preserve anonymity, despite user encryption. In 2013, researchers studied location data from 1.5 million people and found that it was so specific to individual habits that 95 per cent of them could be identified with only 4 spatio-temporal points.39 If contact tracing applications

Figure 4: Privacy spectrum of applications to fight against COVID-19. Inspiration for this visualization comes from about:intel’s blog post on COVID-19 tracking applications.39

Johnny [can] self-report symptoms to get the whole school sent home.38

34 ‘NHS COVID-19: The UK’s Coronavirus Contacts-Tracing App Explained’ (TechCrunch) <https://social.techcrunch.com/2020/05/05/nhs-covid-19-the-uks-coronavirus-contacts-tracing-app-explained/> accessed 11 October 2020.
35 Woodhams (n 15).
36 Michele Loi and others, ‘Ethical Framework for Human-Centric Public Health Digital Surveillance (Public Health Digital Souveillence)’ <https://docs.google.com/document/d/19F_hXIpVdDKC8fTIxN0aexB_GmpFEUuoSUMEj-zY/edit?usp=embed_facebook> accessed 2 July 2020.
37 ‘Will Google’s and Apple’s COVID Tracking Plan Protect Privacy?’ – The Markup <https://themarkup.org/ask-the-markup/2020/04/14/will-gogles-and-apples-covid-tracking-plan-protect-privacy> accessed 14 July 2020.
38 ‘Will Google’s and Apple’s COVID Tracking Plan Protect Privacy?’ (The Markup) <https://themarkup.org/ask-the-markup/2020/04/14/will-gogles-and-apples-covid-tracking-plan-protect-privacy> accessed 14 July 2020.
39 ‘This Window of Opportunism’ (about:intel, 6 April 2020) <https://aboutintel.eu/covid-surveillance-china-europe/> accessed 2 July 2020.
40 Yves-Alexandre de Montjoye and others, ‘Unique in the Crowd: The Privacy Bounds of Human Mobility’ (2013) 3 Scientific Reports 1376.
combine location data with other sensitive information such as banking transactions and social media details, as in Taiwan and South Korea, then there is a higher risk for privacy breaches and even mass surveillance.

Privacy risks also feed the concerns over the establishment of a surveillance infrastructure by governments and large technology companies through digital contact tracing. Caught between the lack of healthcare infrastructure and the risk of socio-economic collapse, some governments such as Colombia, Turkey, and the UK have hastily deployed digital contact tracing solutions without going through democratic and participative approaches centred on informed consent. Many fear such exceptional measures infringing on civil liberties will remain after the pandemic and become ‘the new normal’. Therefore, an effective governance framework is essential to avoid expanding the scope of digital contact tracing applications beyond their initial purposes.

**Stigma and discrimination**

Concerns have been raised about the impact of contact tracing applications on groups who have historically experienced discrimination, stigma, and abuse. There are three significant risks, particularly in countries or companies that use or consider using the data collected from contact tracing applications to make decisions on ‘passporting’ certain services.  

First, the data gathered from contact tracing applications can be used to stigmatize and blame certain individuals. Secondly, there is a risk that insight from location data will be used to stigmatize specific communities or minority groups, such as women, ethnic enclaves (eg Italian or Japanese neighbourhoods), or emerging socio-economic entities (eg food-delivery riders, ride-sharing platform drivers). Third is the risk that groups or individuals avoiding use of contact tracing applications will consequently be denied access to services or entry to certain places.

Digital contact tracing carries an intrinsic risk of stigmatization as it entails collecting data on entire populations. This data can be used outside the purpose of monitoring COVID-19 exposure and lead to singling out coronavirus ‘hot zones’ thus bringing risks of stigmatization of certain neighbourhoods, areas, or even entire regions. Ethnic minority neighbourhoods could become an easy target for stigmatization and discrimination. In addition, front-line and second-line workers such as food delivery riders, cashiers, drivers are more exposed to the virus. If employment in these professions intersect with marginalized groups, the impact of digital contact tracing will be all the more severe for these groups. Stigmatization creates alienation and harms social cohesion. However, the same data that might be used to stigmatize specific groups also serves an essential function in fighting the pandemic’s impact. If certain professions bear the brunt of the risks associated with COVID-19, data collected by contact tracing applications can be helpful to evidence this.

**Accessibility**

To be widely adopted, contact tracing applications also rely on mass access to digital technologies and the corresponding literacy. Without specific measures aimed at proactively bridging the digital divide, user-bases will be limited, and specific subgroups will even be denied service. Although increasingly widespread, access to mobile technology remains incomplete across the world. In 2019, two-thirds of the world’s population did not own a smartphone, and smartphone penetration was only 24 per cent in India and 60 per cent in Brazil and South Africa. Access to sufficient bandwidth is also limited in certain areas, not even to mention the cost of access to broadband connections. Digital literacy is often highly correlated with other socio-economic characteristics: one recent review of Twitter users in Italy found them to be on average younger and more highly educated than the overall population. People with disabilities have also historically suffered from the digital divide. Luciano Floridi has emphasized that it is not only essential to get a certain percentage adoption rate for contact tracing applications to be effective, but that adoption be spread across the population: ‘The app works much better the more it is widespread, and is most widespread where there is more digital literacy and ownership of mobile phones . . . .

---

41 ‘Chez Engie, polemique autour d’une application «anti-Covid» destinée à ses salariés’ Le Monde.fr (14 July 2020) <https://www.lemonde.fr/emploi/article/2020/07/14/chez-engie-polemique-autour-d-une-application-anti-covid_604618_1698637.html> accessed 29 July 2020.
42 COVID-19 Stoking Xenophobia, Hate and Exclusion, Minority Rights Expert Warns’ (UN News, 30 March 2020) <https://news.un.org/en/story/2020/03/1060602> accessed 13 July 2020.
43 677 Huntington Avenue Boston and Ma 02115 +1495-1000, ‘Contact Tracing Apps: Extra Risks for Women and Marginalized Groups’ (Health and Human Rights Journal, 29 April 2020) <https://www.hhrljournal.org/2020/04/contact-tracing-apps-extra-risks-for-women-and-marginalized-groups/> accessed 13 July 2020.
44 Loi and others (n 36).
45 ‘Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally’ (Pew Research Center’s Global Attitudes Project, 5 February 2019) <https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/> accessed 2 July 2020.
46 Cristian Vaccari and others, ‘Social Media and Political Communication: A Survey of Twitter Users during the 2013 Italian General Election’ [2013] Rivista italiana di scienza politica.
47 Elizabeth Rust, ‘How the Internet Still Fails Disabled People’ the Guardian (29 June 2015) <http://www.theguardian.com/technology/2015/jun/29/disabled-people-internet-extra-costs-commission-scope> accessed 14 May 2020.
Therefore, there is a very concrete risk of privileging the already privileged, and their residential areas. The digital divide may become a biological divide.  

**Governance of contact tracing applications**

The scale of these concerns suggests the need of a robust ethics and governance framework to ensure that use of contact tracing technology is underpinned by democratic values, and that governments and the private sector are accountable for uses of this technology. Different governance tools can be involved in the deployment of contact tracing applications, including legal protection of privacy and non-discrimination, impact assessments, audits, certification, and public and institutional oversight. Studies show that public trust and social acceptability play an important role in determining compliance with COVID-19 containment policies. Trustworthy governance is therefore essential for the deployment of contact tracing applications, and can rely on several legal and institutional mechanisms.

**Legal protections**

In several countries where contact tracing applications have been deployed, these technologies are underpinned by legal protections—offering a framework in which the public and private agencies running the applications can work, and creating legal obligations that ensure application developers and operators are accountable to the public. At the very least countries developing contact tracing applications must comply with existing national and regional legislation: here, privacy and non-discrimination frameworks are most relevant. Elsewhere, new legislation has been passed specifically to provide guidelines to the deployment and use of contact tracing applications.

**Existing data privacy regulation**

Data collected through contact tracing applications pertains to private health information, which is governed by existing systems for data protection. However, requirements differ considerably across jurisdictions. While the EU has a comprehensive data protection regulation in the form of the European General Data Protection Regulation (GDPR), data protection varies across Latin America. For example, the Brazilian constitution includes privacy and the protection of communications, alongside a recent Brazilian Supreme Court ruling defining data protection as a fundamental right. To instill trust, digital contact tracing solutions should be developed in line with principles of data protection by design and default. In Brazil these requirements would be covered by the Código de Defesa do Consumidor (Consumer Protection Code) which requires that users of products and services must be provided with adequate information about how the product will be used, and that this must be conveyed in an understandable way.

Data protections should include purpose limitations to avoid the risk of repurposing data by law enforcement or intelligence services. Article 6 of the specific legislation introduced for COVID-19 in Brazil requires that the sharing of essential data regarding the identification of people infected or suspected of being infected with the coronavirus is mandatory between public agencies and entities of any level of the Brazilian federation (federal, state, municipal level and the federal district). There is a significant risk that a blurry interpretation of ‘essential data’ could lead to widespread sharing of personal data.

**Existing non-discrimination regulation**

It is necessary to clarify that even if ‘discrimination’ is on the basis of the analysis of health status, anti-discrimination legislation does not always prohibit the use of contact tracing applications. To explain why, we need to distinguish between acts of differentiating (or neutrally discriminating) and illegally discriminating. In this sense, contact tracing applications operate based on differentiating the health status of their users (eg individuals are either positive or negative to the virus). There is no pejorative value, in and of itself, attributed to this activity. The problem arises when the data collected by these applications is later used to make illegal distinctions between people—for example, when health insurance agents use that data to deny coverage to those who have been infected by COVID-19. When situations like these happen, anti-discrimination legislation bites.

---

48 Luciano Floridi, ‘Mind the App - Considerations on the Ethical Risks of COVID-19 Apps’ (Mind the app - considerations on the ethical risks of COVID-19 apps) <https://thephilosophyofinformation.blogspot.com/2020/04/mind-app-considerations-on-ethical.html> accessed 2 July 2020.

49 Olivier Bargain and Ulugbek Aminjonov, ‘Trust and Compliance to Public Health Policies in Times of COVID-19’ IZA Discussion Paper <https://www.iza.org/publications/dp/13205/trust-and-compliance-to-public-health-policies-in-times-of-covid-19> accessed 13 July 2020.

50 ‘A Framework for Responsible Limits on Facial Recognition Use Case: Flow Management’ (World Economic Forum 2020) <https://www.weforum.org/whitepapers/a-framework-for-responsible-limits-on-facial-recognition-use-case-flow-management/> accessed 13 July 2020.

51 May 6th and 7th 2020, ruling the Medida Cautelar nas Ações Diretas de Inconstitucionalidade n. 6387, 6388, 6389, 6593, 6390

52 Código de Defesa do Consumidor, Atualizada até setembro de 2017, <https://www2.senado.leg.br/bdsf/bitstream/handle/id/533814/4d_c_e_normas_correlatas_2ed.pdf> accessed 13 July 2020.

53 Law no. 13,979/20

54 Translated. See Brazilian Law No. 13,979 of February 6, 2020 for original.
In those cases, existing equalities legislation, for example the UK Equalities Act of 2010, or prohibition of discrimination under Article 14 of the European Convention of Human Rights, provide frameworks and constraints for the development of contact tracing applications and the way they may discriminate against communities. For members of the EU, protections will be available against discrimination that relate to access to employment, welfare or other forms of social security, the supply of goods and services, including housing and access to justice—specific issues covered in EU Non-Discrimination Directives.

Specific regulation around digital contact tracing tools

Sometimes, the introduction of a new technology reveals that existing legislation is inadequate to deal with the risks posed. The ‘gold-standard’ for the governance of applications is to introduce a new piece of legislation around the digital contact tracing tool. Switzerland, Germany, Australia, France, and Austria have all introduced, or will introduce legislation in this area. Factors that have been considered in these legislative pieces include:

- Time-limitation—in France, StopCovid’s press release highlights the temporary nature of the application;
- Application of the legal tests of necessity and proportionality to introduction and use of contact tracing applications;
- Restrictions on the purposes for which applications can be used—in Australia, for example, employers cannot make use of the application a requirement for returning to work;
- Limitation of data collection—for example, the data collected must be no more extensive than that required for controlling the spread of COVID-19.

Other governance mechanisms

In addition to legal safeguards on the use of contact tracing applications, their design, deployment, and maintenance can rely on other forms of governance. Oversight is essential in every phase of the process to build trust. Public involvement in particular should be strongly encouraged. Impact assessment can help align the end-product with ethical and performance objectives. Finally, continuous third-party audits could guarantee that the application’s use is beneficial.

Oversight

Given the deployment scale of digital contact tracing technologies, the WHO has recommended that these projects be subject to an oversight regime that makes sure that they function as intended. Governments can embed mechanisms for rigorous evaluation and independent oversight of the technology to ensure that full impact assessments are carried out prior to introduction, and that the technology is working as intended following introduction. The oversight may be specific to the application, the agency introducing the applications (eg the NHSX ethics board), or relating to a general theme as part of an existing oversight body such as for data protection—for example, the CNIL in France published an extensive opinion on the StopCovid contact tracing application.

Transparency requirements offer a good first step for the governance of technologies. Several countries have taken important steps in this direction when deploying their contact tracing applications—namely, by making their application open source. The code of Poland’s ProteGO, for example, is published on GitHub, and collects comments from developers and testers. Malaysia and Israel have also promised to make their code public, among many others.

Public involvement

Public participation and interaction with policymaking can help improve public trust. To obtain the consent of those who are likely to be required to download the application requires that citizens have a role in testing and overseeing the use of the application. Mechanisms to facilitate this public involvement could include expert involvement from the public health sector, civil society organizations, and representatives of marginalized groups.

Impact assessment

Frequently, determining whether legal protections are adequate and whether additional protections are necessary require a technological impact assessment. A full technological impact assessment, before the deployment

---

55 Equality Act 2010.
56 European Convention on Human Rights.
57 Non-Discrimination Right.
58 Some academics argue that even GDPR, the most extensive set of data privacy protections globally are inadequate to govern the application: Lilian Edwards, professor of law, innovation and society at Newcastle University and member of the Ethics Advisory Board for the NHSX application, says that the Data Protection Act is inadequate and relying on already existing legislation would mean ‘huge amounts of uncertainty’. ‘[The Data Protection Act] is enabling rather than prohibitive – there are very few things that it says you cannot do’.
59 ‘Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing’ (World Health Organization 2020) <https://www.who.int/publications-detail-redirect/WHO-2019-nCov-Ethics-Contact_tracing_apps-2020.1> accessed 13 July 2020.
60 ‘Poland Works on Smartphone App to Help Stop Coronavirus Outbreak’ Reuters (3 April 2020) <https://www.reuters.com/article/us-health-coronavirus-poland-tech-idUSKBN21L24R> accessed 29 June 2020.
61 ‘Reimagining Regulation for the Age of AI: New Zealand Pilot Project’ (World Economic Forum 2020) <https://www.weforum.org/whitepapers/reimagining-regulation-for-the-age-of-ai-new-zealand-pilot-project/> accessed 29 July 2020.
of any digital contact tracing application, would determine whether any public interests are threatened, and whether existing legislation is adequate to safeguard interests. In the UK, even the narrow, data-protection focused impact assessment (DPIA), required under GDPR, enabled issues to be identified at an early stage. The extensive scope of the data collected through the applications suggests that impact assessments are necessary to determine the short and long-term consequences—societal, economic, ethical, and legal—of new technologies. Understanding the impacts at each of these different levels helps to build public understanding of the application of these technologies, and reduce concerns about the lack of transparency.

Third-party audit
Review by independent bodies can also help to enhance accountability. The audit framework should aim to assess the effectiveness of the application against technical, ethical and policy ambitions, and to present these assessments to those that manage the application. The presence of an independent third party to conduct an external audit should help to enhance oversight.

The case for an ethical framework
In addition to legal protections and governance mechanisms, the adoption of an ethical framework is a complementary strategy, for several reasons. Since contact tracing applications are a new phenomenon, there are few well-established legal frameworks on the subject. Many countries do not have standards, and even those that do still argue about the correct interpretation and adaptation of these tools in the context of contact tracing. Since ethical principles are instead based on common values, we choose to focus on such a framework. From the basis of our Ethical Framework, each country can make the necessary adaptations to incorporate these ideas into their legal environment. New governance strategies include soft legal tools that can deal with new situations on an experimental basis. They are flexible, result-oriented, and likely to be reconsidered if non-beneficial. This makes them apt at tackling unforeseen challenges such as COVID-19, where risks are still largely unknown.

Methodological pathway for the trustworthy adoption of digital contact tracing
It is the collective responsibility of public health authorities and digital experts to develop an ethical and legal framework to help navigate tensions between public health, safety, economic activity, and civil liberties. The urgency of the situation should not impact the capacity to build a comprehensive framework guiding citizens, application developers and policymakers’ choices. We strongly believe that informed individuals are more willing to accept potentially significant but necessary sacrifices when these are self-imposed and ethically justified. Building a trustworthy Ethical Framework is therefore key to ensure social cohesion and contact tracing applications’ effectiveness. In this section, we present an Ethical Framework that we have developed to evaluate digital contact tracing applications.

The goal of the Ethical Framework is to serve as the main reference for civil society, application developers and policymakers, among others, when assessing the ethical risks and benefits raised by digital contact tracing solutions. The principles have been drafted to be action-oriented, with a criteria assessment list associated with each principle, to allow for the continuous evaluation of contact tracing applications. This allows for the systematic evaluation of digital contact tracing applications with respect to privacy-by-design, voluntariness of use, non-stigmatizing, among other principles.

This article presents several contributions. First of all, the Ethical Framework builds on existing literature for the trustworthy adoption of AI systems and other emerging technologies. These include multi-stakeholder ethical frameworks for trustworthy AI adoption built by the Organisation for Economic Co-operation and Development (OECD), the EU High-Level Group, and Institute of Electrical and Electronics Engineers (IEEE); ethical guidelines for digital health applications in times of pandemic drafted by independent regulatory bodies (such as the French Data Protection Agency CNIL or academic labs (such as the University of Zurich); and actionable principles developed for specific use cases like the World Economic Forum’s framework for Facial Recognition.

62 Paul Nemitz, ‘Constitutional Democracy and Technology in the Age of Artificial Intelligence’ (2018) 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20180089.
63 Under Article 35, DPIAs must consider all ‘risks to the rights and freedoms of natural persons’. In practice, however, DPIAs have usually been confined to data protection.
64 Contact-Tracing App Data “Could Feed into NHS Covid-19 Data Store” (Digital Health, 11 June 2020) <https://www.digitalhealth.net/2020/06/contact-tracing-app-data-could-feed-into-nhs-covid-19-data-store/> accessed 13 July 2020.
65 David Banta, ‘What Is Technology Assessment?’ (2009) 25 Suppl 1 International Journal of Technology Assessment in Health Care 7.
66 OECD Legal Instruments, Recommendation of the Council on Artificial Intelligence 2019.
67 European Commission, ‘Ethics Guidelines for Trustworthy AI’ (2018) Text <https://ec.europa.eu/futurium/en/ai-alliance-consultation/> accessed 22 October 2020.
68 IEEE SA, ‘IEEE Ethics In Action in Autonomous and Intelligent Systems’ (2019) <https://ethicsinaction.ieee.org/> accessed 22 October 2020.
69 Marie-Laure Denis, Deliberation N°. 2020-046 of April 24, 2020 delivering an opinion on a proposed mobile application called ‘StopCovid’ 2020 10.
70 Kerstin Noelle Vokinger and others, ‘Digital Health and the COVID-19 Epidemic: An Assessment Framework for Apps from an Epidemiological
Technologies. In some cases, these ethical principles, such as 'privacy by design' and 'minimal use of data and technology', are underpinned by existing legal frameworks such as the EU Law for the GDPR. However, these principles are put into a new perspective in light of the pandemic and digital contact tracing applications.

Our second main contribution is the Criteria Assessment Grid. Its goal is to evaluate all contact tracing applications, whether they are already deployed or under development. The actionable questionnaire directly derived from the Ethical Framework aims at helping application developers, public health authorities and citizens to monitor the trajectory of contact tracing applications. This understanding will collectively guide society in whether or not they want to implement technological solutions, and if so, under which conditions and with which strategy.

### Chart of ethical principles

| I. Performance, Purpose, and Effectiveness |
|------------------------------------------|
| The purpose of applications should be clear, explained in the broader context, measurable and independently auditable. |

| II. Voluntariness and reversibility |
|-----------------------------------|
| Individuals must be free to choose to install the application, with no negative consequences if they choose not to. Users should be able to deactivate the application temporarily or permanently at all time. |

| III. Privacy by design |
|------------------------|
| Contact tracing applications should achieve the highest levels of privacy protection. Data storage should be secure and pseudonymized. |

| IV. Minimal use of data and technology |
|---------------------------------------|
| Data collection must be proportionate, justified, and with a defined expiration date. Only minimal data necessary to fulfil the application’s purpose should be used and stored. |

| V. Transparency and verifiability |
|----------------------------------|
| The complete source code for the application and core tracing protocol must be freely available and reproducible, without access restrictions, for audits. |

| VI. Non-discrimination and non-stigmatization |
|-----------------------------------------------|
| Application developers and policymakers should ensure that contact tracing applications do not stigmatize against people tested positive and their relatives, against categories of social workers, against neighbourhoods, and against people who do not wish to use the application. |

| VII. Accessibility |
|-------------------|
| It should be recognized that smartphone applications and internet connection are not accessible for the entire population. Complementary and alternative solutions should be developed to ensure accessibility. |

| VII. Notice and informed consent |
|---------------------------------|
| Information on the application’s purpose, features, and data collection, should be clearly presented to the user. Informed and explicit consent should be a prerequisite. |

| IX. Accountability |
|--------------------|
| Contact tracing applications must be continuously evaluated and audited by legitimate independent entities. All parties involved in the design and deployment should be accountable through clear legal frameworks of penalties and responsibilities. |
Criteria assessment grid

I. Performance, purpose, and effectiveness
• Was the contact tracing application designed within a broader public health strategy (eg available masks, compliance with social distancing measures and self-isolation, etc.)? What were the other public health measures taken?
• Is there a mission statement or white paper defining the purpose of the application?
• Is the purpose of the application expressly limited? Limitations can be provided by legislation, oversight, or other accountability measures.
• Is there an ‘exit strategy’ for the application in case it has filled its purpose or lacked effectiveness to achieve its purpose

II. Voluntariness and reversibility
• Is the application entirely voluntary?
• Do additional features on the application incentivize or nudge users to sign up, and are these services available elsewhere? (eg self-monitor symptoms, find stores with available mask supplies, etc.)
• Do existing users have the option to temporarily or permanently delete the application, along with all their user information?

III. Privacy by design
• Were privacy factors considered when designing the application, including the data collection and the data storage protocols?
• If applications are developed using more intrusive GPS schemes, are additional steps taken to protect user data such as pseudonymization?
• Is the data shared with any third parties? Is this clearly indicated in the terms of reference and can users opt-out?

IV. Minimal use of data and technology
• What type of location data is collected? What type of health data is collected? What other data is collected?
• Is the use of data by the contact tracing application justified by the application’s mission statement, and coherent with the gravity of the health crisis?
• What kind of analyses are conducted in addition to contact tracing? Are transparent with the users, and consistent with the application’s mission statement?
• How long is data stored for?

V. Transparency and verifiability
• Are the conditions of data collection, storage, and destruction clear to users?
• Is the application’s design, objectives, and use understandable by users? The application’s mission statement should be provided in concise, clear and unambiguous language.
• Is the application open source? Is source code available on a platform that supports comments and feedback?

VI. Non-discrimination and non-stigmatization
• Has special attention been given to the possible inferences people could draw from the data and from how the application communicates on it?
• Could the application encourage discrimination against any categories of social workers (eg emerging social identities such as food delivery and car sharing drivers)?
• Could the applications encourage discrimination against any specific neighbourhoods (eg zones identified as a cluster)?
• Is the application also used for passporting (eg to enable people to claim benefits or to return to work)?

VII. Accessibility
• Has the application deployment accounted for the limited digital access of certain population groups (eg the disabled, elderly, or less tech-savvy)?
• Have there been any specific measures introduced to mitigate this accessibility gap?
• Are the services provided by the application available otherwise?

VII. Notice and informed consent
• Are users asked for their consent at setup?
• Are there any dark patterns in how the application works? Dark patterns can include nudges via push notifications, by-default installation of the application on smartphones, hidden features to deactivate or remove the application, etc.

IX. Accountability
• Are there independent assessments and oversights? Can the public place their full trust in these organizations?

72 ‘Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing’ (n 58).
How was the general public involved in the design and deployment of the application?

Are application developers held accountable both internally and externally? Is the general public involved in this? The WHO’s definition of contact tracing accountability includes that ‘individuals must be given the opportunity to know about and challenge any measures to collect, aggregate, retain and use their data’.73

Regarding data collection, who is able to gather and use the data which is collected? What decisions are made on the basis of the data which is collected? How is this data analysed and in combination with which other data sources? Is this consistent with the principles of data minimization and proportionality?

Regarding decision-making, who can make decisions about the use and governance of the application? How are these decisions made? Who can challenge these decisions?

**Applications and conclusion**

Studying existing applications through the lens of this framework highlights a wide range of strategies adopted by different national governments. A number of watchdogs have called out the most intrusive ones, including the applications of Kuwait and Bahrain, but also Norway’s now-suspended programme and China’s secretive contact-tracing efforts.74 Other applications have been deployed, to varying degrees of compliance with our privacy and voluntariness criteria (see Figure 5). In some cases, insufficient technical safeguards drive public scepticism: Colombia’s CoronApp was vastly criticized upon deployment and has not been widely installed to this day. However, the relative failure of the first version of France’s StopCovid highlights that even applications that aim for the highest levels of voluntariness and privacy can see failed implementation. There, the lack of clear oversight body and public engagement crystallized tensions and resulted in low adoption.

The case of Latin America is of particular interest: initially low numbers have recently given way to record highs across the continent. Almost all Latin American national and some sub-national governments have introduced technologies for combatting COVID-19.75 Introduction of these applications is made particularly complex in Latin America where up to 45 per cent of

---

73 Ibid.
74 ‘Bahrain, Kuwait and Norway Contact Tracing Apps a Danger for Privacy’ (n 21).
75 ‘Lo que las aplicaciones de seguimiento de contactos no pueden hacer por los gobiernos’ (CAF Banco de Desarrollo de América Latina) <https://www.caf.com/es/conocimiento/visiones/2020/05/lo-que-las-aplicaciones-de-seguimiento-de-contactos-no-pueden-hacer-por-los-gobiernos/> accessed 14 July 2020.
the population do not have access to active internet connection\textsuperscript{76}; to support accessibility, the Colombian government has given free internet access.\textsuperscript{77} These applications vary in their functionality, reflecting the different needs of the population, but most are limited to basic services information (Brazil), symptom evaluation (Argentina), or both (Chile). Some countries have unsuccessfully deployed contact tracing features: in Colombia, the official application’s contact tracing functionality was deactivated due to security concerns.\textsuperscript{78} Only Peru has deployed a contact tracing application, called ‘Perú en tus manos’.\textsuperscript{79} The application collects both Bluetooth and GPS records, and the Terms of Use state that all data collected is stored on central Google servers.

The epidemiological characteristics of COVID-19, and the way it has rapidly spread across the world, make digital contact tracing applications a valuable tool in a country’s response to the pandemic. However, given the extent of the ethical issues at hand in the design, deployment, and day to day operations of such applications, it is our collective responsibility to build solid ethical and governance frameworks to make informed choices. Key to these decisions are the objectives of cultivating public trust and raising public awareness—both of which are essential to an application’s wide adoption and success. In this article, we have provided an overview of governance mechanisms as well as an ethical framework and a number of criteria on which to evaluate contact tracing applications—be they already launched or still in development. More generally, governing bodies should be cautious of technosolutionism as a way out of crisis: only a balanced combination of technological and public health measures, voluntarily adopted by an informed public, can help us fight against COVID-19.

doi:10.1093/idpl/ipab001

\textsuperscript{76} ‘Construyendo un milagro digital para todos’ (CAF Banco de Desarrollo de América Latina, 2 July 2019) <https://www.caf.com/es/conocimiento/ visiones/2019/07/construyendo-un-milagro-digital-para-todos/> accessed 14 July 2020.

\textsuperscript{77} Tomás Betín, ‘Descargar CoronApp Colombia dará internet y minutos gratis durante un mes’ El Heraldo (24 April 2020) <https://www.elheraldo.co/colombia/descargar-coronapp-colombia-dara-internet-y-minutos-gratis-durante-un-mes-720660/> accessed 14 July 2020.

\textsuperscript{78} ‘Colombia had to abandon contact tracing from its coronavirus app because it didn’t work properly’ (Business Insider France, 7 May 2020) <https://www.businessinsider.fr/us/colombia-contact-tracing-apple-google-coronavirus-app-2020-5/> accessed 14 July 2020.

\textsuperscript{79} ‘Gobierno lanza nueva versión de app “Perú en tus manos” para advertir a los ciudadanos sobre las zonas con mayor probabilidad de contagio’ (GOB.pe, 7 May 2020) <https://www.gob.pe/institucion/pcm/noticias/150943-gobierno-lanza-nueva-version-de-app-peru-en-tus-manos-para-advertir-a-los-ciudadanos-sobre-las-zonas-con-mayor-probabilidad-de-contagio/> accessed 14 July 2020.