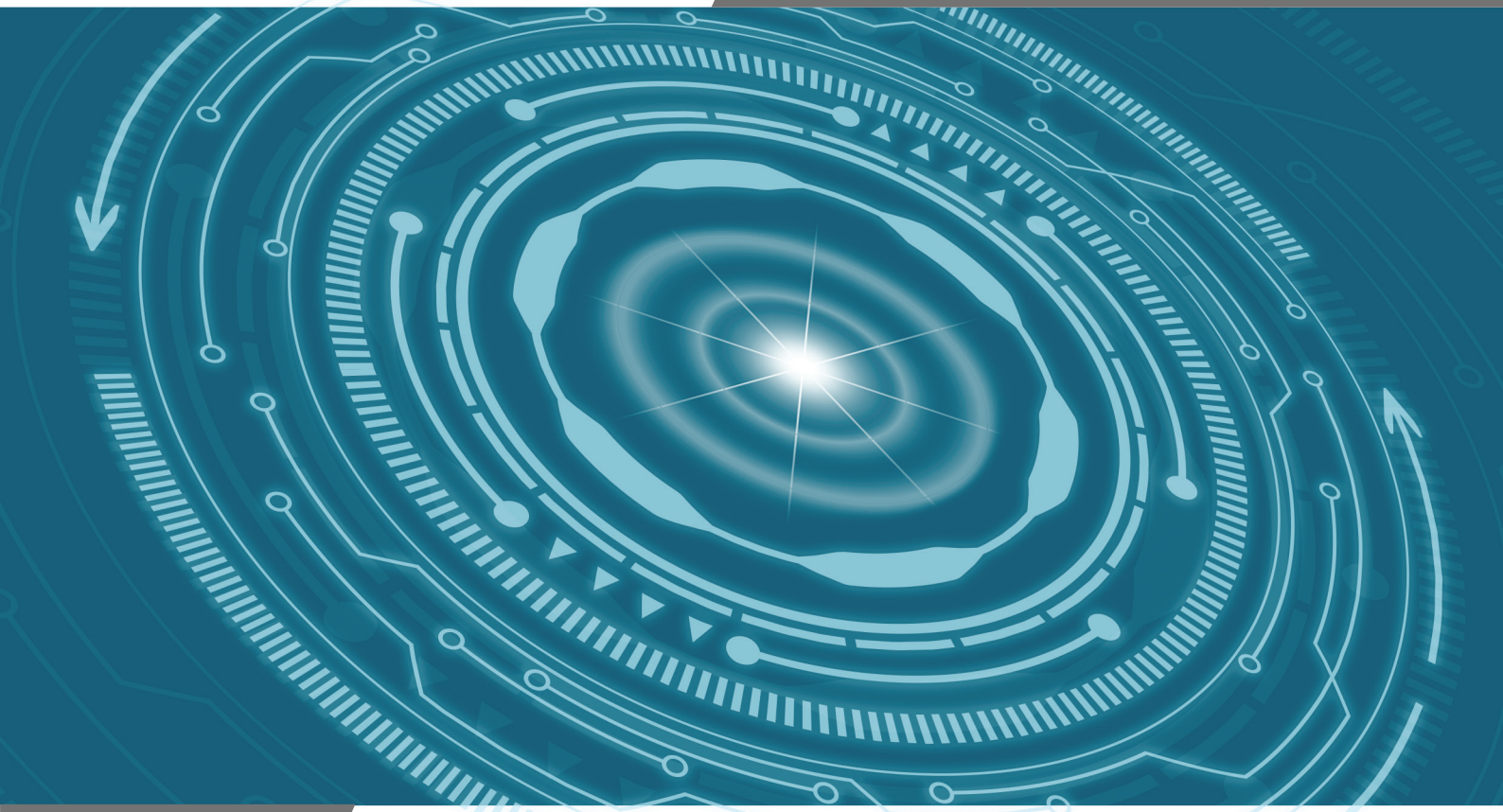
Centre for Economics and Foreign Policy Studies

edam

Cyber Governance and Digital Democracy 2020/05/EN



June 2020

SAFETY AND PRIVACY IN THE TIME OF COVID-19: CONTACT TRACING APPLICATIONS

Emre Kursat Kaya | Research Fellow

SAFETY AND PRIVACY IN THE TIME OF COVID-19: CONTACT TRACING APPLICATIONS

Emre Kursat Kaya | Research Fellow

I. Introduction

As the number of global COVID-19 confirmed cases passed 5 million, public and private actors are continuing to take measures to contain the pandemic[1]. The biggest sanitary crisis of the last century has already claimed 324,000 life.
Government actions have varied from one country to another. While some countries have chosen to apply strict lockdowns, others have adopted *laissez-faire* attitudes. Yet, a common denominator for containing the spread of the virus has been the use of a trio of non-pharmaceutical interventions: social distancing, testing, and contact tracing for infected individuals.

While there are significant scientific and political debates on both social distancing rules and the number of testing, this paper focuses on contact tracing applications (apps). Contact tracing provides authorities information required to identify anyone who has been in relatively close contact with the subject individual. Health authorities widely use this instrument to create the list of at-risk individuals who a certain patient has been in contact with. Traditionally, manual contact tracing has been the most widely used method. It consists of interviews, CCTV footage analysis, credit card usage history and other labor-intensive/time-consuming activities.

Digital contact tracing has been put forward by public authorities to automatize and accelerate the process[2]. In most cases, the system requires the use of a smartphone to function. Currently, there is no universally adopted contract tracing method. Developed apps differ in several aspects. The main divergences are regarding the use of GPS location or Bluetooth data and the centralized or decentralized storage of data. The different models and their use in practice will be described in the second part of this paper.
Regardless of the type of application adopted, there are two large debates around the use of these digital tools to increase the safety of citizens. The first debate is about the efficacy of these apps. Are they game-changers? What is their potential impact on the fight against the virus? Effectiveness is an umbrella prerequisite that will be further fractioned in this paper.

The second debate regarding the widespread use of these apps is around privacy issues. What kind of data will these apps collect? Which are the measures to take to safeguard personal data? Is there a risk of mission creep? As for any policy intervention, and especially for one which suggests a trade-off between safety and privacy, a proportionality test must be envisaged.

FRIEDRICH NAUMANN FOUNDATION For Freedom. Turkey

This research has been made possible by funding obtained from the Germany-based Friedrich Naumann Stiftung's "Liberal Homeworks Online" project.

1 John Hopkins University, COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE), retrieved May 22, 2020, from https://coronavirus.jhu.edu/map.html

2 Ferretti, L. & al. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing, Science, retrieved May 19, 2020, from https://science.sciencemag.org/content/368/6491/eabb6936

II. Contact-Tracing Applications

Both at academic and policymaking levels, there is no consensus on the most useful type of digital contact-tracing applications. Researchers have suggested several criteria to differentiate the existing apps[3]. Many of these conditions such as the existence of a sunset clause that would limit the use of the app to fighting the COVID-19 are widely accepted. Voluntary use and minimum-data approaches are generally promoted criteria. Two key aspects of contact-tracing apps stimulate much attention. These are data collection and data storage methods.

GPS-Location Data

The discussions on data collection methods are focused on the use of GPS-location data or Bluetooth Low Energy (LE). GPS-location has the advantage to also signal possible non-human transmissions such as via a restaurant table or an industrial machine used by another colleague[4]. An additional advantage of such a method is that it does not require the extra use of battery as an active GPS is sufficient[5]. However, location-based contact tracing raises significant privacy issues. Thus, as it will be demonstrated below, most democratic governments do not favor it.

Bluetooth Low Energy Data

Bluetooth-based contact tracing applications are more common and will possibly become the norm. Following the example set by Singapore's TraceTogether[6], more and more countries are opting for the use of Bluetooth tech. With this method, individuals download an application that will detect other smartphones' Bluetooth signals and record their randomly generated anonymous code. The advantage of using Bluetooth technology is that thanks to the Received Signal Strength Indication (RSSI), it can adequately determine the proximity and duration of an interchange. For instance, with this technology, a device can perceive obstacles such as walls or floors. When an individual is COVID positive, the system sends a notification to all individuals who have been in close contact (i.e. less than 2m for more than 10min) with the patient. These at-risk individuals are then asked to test and/or to go into quarantine. This method is regarded as the most privacy-friendly one as the data shared is very limited and at least on theory, it is highly difficult to identify involved individuals. Yet, there are security disadvantages. Indeed, Bluetooth technology is highly vulnerable to hacking[7]. As part of a largescale update in January, Apple has solved four Bluetooth bugs out of five patches in total[8].

Centralized Model of Data Storage

The data storage issue is as important as data collection when it comes to efficacy and privacy. Centralized and decentralized data storage are the two models used for contact tracing apps. In the centralized model, public authorities are collecting data in a central server where the matching between data is made. Arguably, this offers a better epidemiological use of the data. Yet, privacy advocates insist that a centralized model has a higher risk of mission creep and is more vulnerable to hacking.

Decentralized Model of Data Storage

In the decentralized model, the unique codes created through a contact event are recorded on each individuals' device and are not transmitted to a central server. The data can be processed only when one of the users is infected. Its content is restricted to individuals the patient has been in close contact with. By creating smaller data clusters, the decentralized model offers better protection against large-scale malicious activities or government abuses (i.e. creation of social graphs). This model has been mostly promoted through the cooperation between Apple and Google to create an Application Programming Interface (API)[9].

---

3 An example of list of criteria: O'neill, P.H., Ryan-Mosley, T & Johnson, B. A flood of coronavirus apps are tracking us. Now it's time to keep track of them, MIT Technology Review, retrieved May 19, 2020, from https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/

4 Greenberg, A. Clever Cryptography Could Protect Privacy in Covid-19 Contact-Tracing Apps, Wired, retrieved May 19, 2020, from https://www.wired.com/story/covid-19-contact-tracing-apps-cryptography/

5 Berke, A., & al. Assessing Disease Exposure Risk with Location Data: A Proposal for Cryptographic Preservation of Privacy, MIT.

6 For more details on TraceTogether: https://www.tracetogether.gov.sg/

7 PhoenixTS, Hacking Bluetooth Devices: Bluebugging, Bluesnarfing, and Bluejacking, retrieved May 20, 2020, from https://phoenixts.com/blog/hacking-bluetooth-devices-bluebugging-bluesnarfing-bluejacking/

8 Reynolds, C. Google Continues to Prod Holes in Apple's Security, Computer Business Review, retrieved May 20, 2020, from https://www.cbronline.com/news/apple-cves-google

9 Apple & Google, Privacy-Preserving Contact Tracing, retrieved May 19, 2020, from https://www.apple.com/covid19/contacttracing

	Excessive Data Collection	Limited Data Collection
High risk of mission creep and/or hacking	Centralized GPS-Location Data	Centralized Bluetooth Data
Low risk of mission creep and/or hacking	Decentralized GPS-Location Data	Decentralized Bluetooth Data

Table 1: *Models of Contact Tracing Application*

Apple/Google Privacy-Preserving Contact Tracing API

An API is not an application per se, but rather a framework to facilitate the use of Bluetooth technologies on Android and iOS operating smartphones for public health authorities. Based on this framework, every national/regional contact tracing application will have its own features.

On May 20, 2020, Apple and Google launched the first version of their API, named the Exposure Notification system[10]. Now public health authorities around the world will be able to use this software to develop more accurate and rapid contact-tracing applications. For privacy concerns, the two tech giants have forbidden the use of the app to any GPS/location-based software[11]. The companies went also further regarding the protection of Bluetooth data by encrypting all the metadata.

Apple and Google have also announced that several U.S. states and 22 countries have approached them to use the API during the development phase[12]. These countries are the ones opting for the decentralized Bluetooth-based model. It is worth noting that, the two companies aim to limit the use of the software to one official or quasi-official application by country[13]. This policy aims at limiting the spread of both commercial and malicious apps. It is yet to be seen if this policy will be fully enforced in countries where contact tracing apps are developed at the subnational level such as the United States or Canada.

10 Apple & Google, Exposure Notification API launches to support public health agencies, retrieved May 21, 2020, from https://blog.google/inside-google/company-announcements/apple-google-exposure-notification-api-launches/

11 Nellis, S. & Dave, P. Apple, Google ban use of location tracking in contact tracing apps, Reuters, retrieved May 21, 2020, from https://www.reuters.com/article/us-health-coronavirus-usa-apps/apple-google-ban-use-of-location-tracking-in-contact-tracing-apps-idUSKBN22G28W

12 Kelion, L. Apple and Google release marks 'watershed moment' for contact-tracing apps, BBC, retrieved May 21, 2020, from https://www.bbc.com/news/technology-52740131

13 Etherington, D. Apple and Google launch exposure notification API, enabling public health authorities to release apps, TechCrunch, retrieved May 21, 2020, from https://techcrunch.com/2020/05/20/apple-and-google-launch-exposure-notification-api-enabling-public-health-authorities-to-release-apps/

III. Who's Using What?

Unsurprisingly, the first countries to introduce contact-tracing applications were countries that were first affected by the COVID-19. China, Hong Kong, and South Korea have developed applications based on a centralized GPS-location-based model. These three countries have seconded digital contact tracing with the analysis of credit card records and CCTV footage[14]. While there is no evidence regarding the role these applications played in the flattening of the respective infection curves of these countries, their invasive nature has been an issue of concern. It is worth noting that the Chinese app is mandatory and is based on QR-code assignment system[15]. Israel is another country that has been heavily criticized for its contact tracing practices. The Israeli government had mandated the Shin Bet, its domestic intelligence service, to monitor phone-location data of COVID patients without their consent[16]. On April 26, the Israeli High Court has banned the use of contact tracing on the ground that the existing method violated the right to privacy. The Israeli Health Ministry has since developed HaMagen, a relatively more privacy-friendly decentralized GPS/location-based application.

Singapore has been the first country to introduce a Bluetooth-based application for contact tracing. The Singaporean TraceTogether app collects Bluetooth data into a central computer. So far, only around 20% of Singaporeans have downloaded the app.

In Europe, despite the European Commission's recommendation on the development of an interoperable application, countries have adopted different models[17-18]. While most European countries have decided to use Bluetooth data, there is a clear divergence regarding data storage. Countries such as the United Kingdom, France, and Norway (the first European country to develop a contact tracing app) adopted the centralized model of data storage[19]. They argue that decentralized data will impede the work of health authorities to follow the spreading trends of the virus[20]. Paris and London are now negotiating with Apple and Google to be able to use their interfaces for their centralized apps. So far, the two tech giants have refused these calls on the ground of privacy concerns. French Digital Minister added that their centralized approach is also a question of sovereignty[21]. Germany's app was initially planned to collect data into a central server. Following public outcry, Berlin has now opted for the Apple/Google-backed decentralized model and joined countries such as Italy, Austria or Ireland.

14 McCurry, J. Test, trace, contain: how South Korea flattened its coronavirus curve, The Guardian, retrieved May 20, 2020 from https://www.theguardian.com/world/2020/apr/23/test-trace-contain-how-south-korea-flattened-its-coronavirus-curve

15 Mozur, P., Zhong, R. & Krolik, A. In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags, The New York Times, retrieved May 21, 2020, from https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

16 Privacy International, Israel: Security service may use patients' smartphone data for contact tracing, retrieved May 19, 2020, from https://privacyinternational.org/examples/3423/israel-security-service-may-use-patients-smartphone-data-contact-tracing

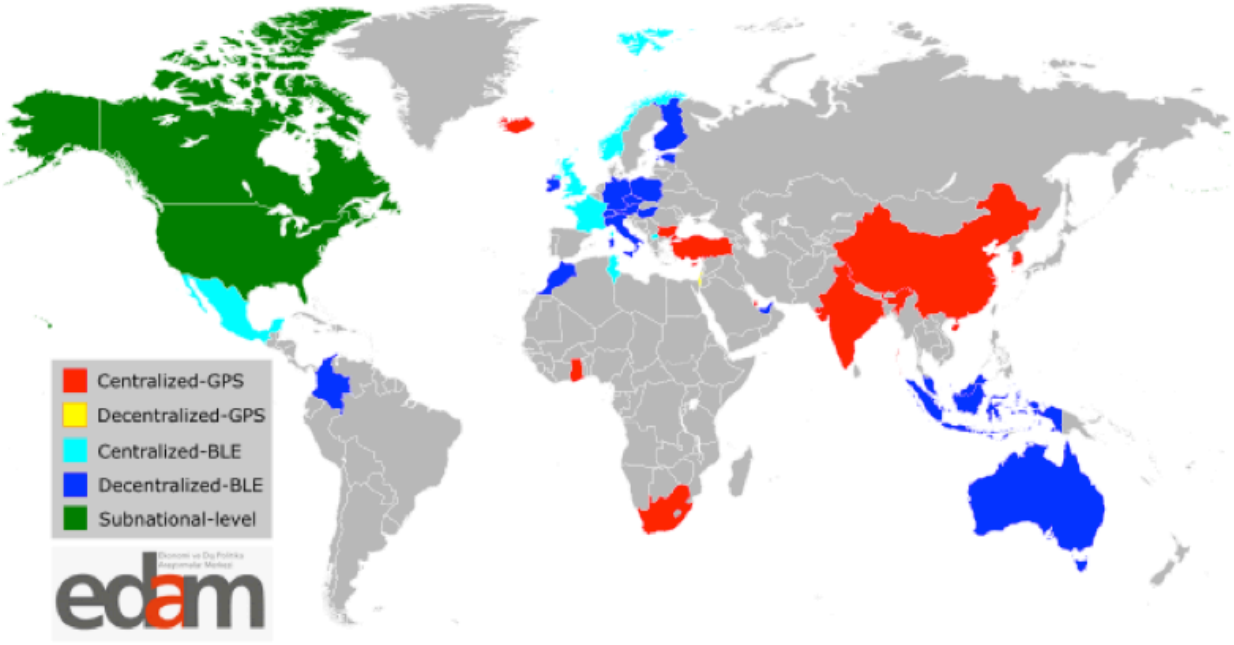
17 European Commission, COMMISSION RECOMMENDATION of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data, retrieved May 20, 2020, from https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf

18 Abboud, L., Miller, J. & Espinoza, J. How Europe splintered over contact tracing apps, Financial Times, retrieved May 21, 2020, from https://www.ft.com/content/7416269b-0477-4a29-815d-7e4ee8100c10

19 Chowdhury, H., Field, M. & Murphy, M. NHS contact tracing app: how does it work and when can you download it? The Telegraph, retrieved May 20, 2020, from https://www.telegraph.co.uk/technology/2020/05/20/nhs-app-uk-coronavirus-contact-tracing-download-when/

20 Vincent, J. Without Apple and Google, the UK's contact-tracing app is in trouble, The Verge, retrieved May 20, 2020 from https://www.theverge.com/2020/5/5/21248288/uk-covid-19-contact-tracing-app-bluetooth-restrictions-apple-google

21 Thompson, R. & Bock, P. StopCOVID: France's controversial tracing app ready by June, government says, Euronews, retrieved May 21, 2020, from https://www.euronews.com/2020/04/29/coronavirus-french-mps-approve-covid-19-tracing-app-despite-privacy-concerns



Map 1: *COVID-19 Contact Tracing Applications Launched or To Be Launched (TBL) by Model*[22]

The United States did not opt for a federal-level contact tracing application. Individual states are responsible for developing their own software. North and South Dakota were the first two states to launch their contact tracing apps, Care19[23]. The software is based on anonymized GPS-location data. The third state to develop a contact tracing application has been Utah. The Health Together app uses both GPS-location and Bluetooth data[24]. Unlike Care19, this app is not anonymized with public health officials having access to identity information. While several other states are planning to launch their contact tracing apps based on the Apple/Google API soon, others are allocating more resources to traditional contact tracing[25]. For instance, New York City is planning to hire 1000 contact tracers.

Turkey is yet to develop its public contact tracing application. Ankara has already launched an information and quarantine surveillance application, Hayat Eve Sığar. The application is highly intrusive as it requires enabling access to an extensive amount of data such as GPS location, camera, Bluetooth, and contacts[26]. Additionally, Ankara opted for a centralized data storage model. Despite its potential invasive nature, the app has been downloaded more than 5 million times or by 6% of the population[27]. Turkish authorities are now planning to incorporate a contact tracing mode to the app similar to the Chinese QR code system[28].

22 Please check the table in the Annex for the detailed list of countries.

23 Setzer, E. Contact-Tracing Apps in the United States, Lawfare, retrieved May 20, 2020, from https://www.lawfareblog.com/contact-tracing-apps-united-states

24 Utah.gov, Healthy Together App, retrieved May 20, 2020, from https://coronavirus.utah.gov/healthy-together-app/

25 Vogelstein, F. & Knight, W., Health Officials Say 'No Thanks' to Contact-Tracing Tech, retrieved May 20, 2020, from https://www.wired.com/story/health-officials-no-thanks-contact-tracing-tech/

26 Kasapoglu, Ç. Koronavirüs: Türkiye ve dünyadaki temas takip uygulamaları güvenli mi, hak ve mahremiyet ihlallerine yol açar mı? BBC Türkçe, retrieved May 21, 2020, from https://www.bbc.com/turkce/haberler-dunya-52638919

27 Yanık, T. & Günyol, A., 'Hayat Eve Sığar' uygulaması 5 milyonun üzerinde indirildi, Anadolu Ajansı, retrieved May 21, 2020, from https://www.aa.com.tr/tr/turkiye/hayat-eve-sigar-uygulamasi-5-milyonun-uzerinde-indirildi/1831032

28 Ibid.

IV. Debate No.1: Effectivity

The debate on the effectivity of contact tracing applications starts at whether they are needed at all. Digital contact tracing has obvious efficiency advantages compared to the labor-intensive manual methods. Yet, there is a quasi-consensus that digital contact tracing is useless as a standalone method. It must be incorporated into a larger manual contact tracing effort involving techniques such as interviews and CCTV analysis. This can partly explain the success of the South Korean experience with contact tracing. Yet, even then, contact tracing is just an instrument among many others in the fight against the pandemic and not a magical solution[29].

A crucial issue regarding the efficacy of a contact tracing application is how widely it is used. A large enough portion of the population must use it. Oxford University's Big Data Institute developed a model to calculate the minimum user percentage required. To stop the spread of the virus, at least 60% of the population must download the app[30]. This does not mean that any lower rate will bring no benefit. The spread of the virus will be slowed if 20% of the population downloads the contact tracing software. As an example, only 19% of Singaporeans have downloaded TraceTogether[31]. So far, the Turkish information and quarantine tracing application has been downloaded by 6% of the population. To increase the number of users, the authorities must offer convincing arguments that they are both useful and trustworthy[32].

However, even the greatest efforts by app developers to persuade users might not be sufficient. For a large majority of the developed apps, the basic requirement is to have a smartphone. Even in developed countries such as the United States or Germany, the smartphone penetration rate is around 80%[33]. South Korea is the only country with more than 90% of smartphone users. Thus, millions of individuals will not be able to use contact tracing apps. It happens that the ones not owning a smartphone are generally in the most vulnerable segment of the population. For instance, +65 persons are less likely to use a phone compatible with the apps. On a global scale, the digital divide is even more concerning. Only 3.5 billion individuals have a smartphone[34]. This is less than half of humankind.

Several tech companies are working to offer solutions that will increase the number of potential users and the time they use the apps. Apple is reportedly working to enable its devices to keep Bluetooth active in the background, something not possible today. The Apple/Google API has been hailed for low battery consumption. Battery longevity is an important effectiveness criterion as a smartphone out of battery cannot be traced. Microshare, a data management company from Philadephia, has developed an affordable contact tracing solution using Bluetooth-based bracelets[35]. The company argues that they developed the Universal Contact Tracing system to be used in factories, warehouses, and other locations where the use of smartphones is limited or prohibited. The consulting firm PwC is developing an app that will enable employers to contact trace their employees and warn them when at risk[36]. While increasing safety at work, these apps can easily become a surveillance instrument by malevolent employers.

29 Soltani, A., Calo, R. & Bergstrom, C., Contact-tracing apps are not a solution to the COVID-19 crisis, Brookings, retrieved May 21, 2020, from https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/

30 Big Data Institute, Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown, Oxford University, retrieved May 21, 2020, from https://www.bdi.ox.ac.uk/news/digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown

31 Hui, M. Singapore wants all its citizens to download contact tracing apps to fight the coronavirus, Quartz, retrieved May 20, 2020, from https://qz.com/1842200/singapore-wants-everyone-to-download-covid-19-contact-tracing-apps/

32 Nature, Show evidence that apps for COVID-19 contact-tracing are secure and effective, retrieved May 20, 2020, from https://www.nature.com/articles/d41586-020-01264-1

33 Statista, Smartphone ownership rate by country 2018, retrieved May 21, 2020, from https://www.statista.com/statistics/539395/smartphone-penetration-worldwide-by-country/

34 Statista, Number of smartphone users worldwide from 2016 to 2021, retrieved May 20, 2020, from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

35 Microshare, Universal Contact Tracing, retrieved May 20, 2020 from https://www.microshare.io/universal-contact-tracing/

36 Financial Times, Private sector races to build virus apps to track employees, retrieved May 20, 2020, from https://www.ft.com/content/caeb250b-8d8b-4eaa-969c-62a8b58464aa

Citizens will need to trust their governments. Vice-versa, public authorities will have to trust the app users too. They will need to trust that people will report their symptoms at an early stage of the infection, if not at all. If there too many cases of false negatives, the population will lose both trust and interest in the app.

There are even bigger risks concerning false positives. Firstly, trolls or simply panicked individuals might falsely report transmission. A simple solution for public authorities would be to require the approval of health care workers to declare infection. Covid-Watch, for instance, would require the user to get a confirmation code from a health care provider[37]. Secondly, there is a risk of malicious reporting. These reportings could aim at destabilizing the economy and impeding public trust towards authorities. Finally, and as a combination of the previous points, the repetition of false positives could create a "crying wolf" effect and undermine the overall effectivity of the application.

V. Debate No.2: Privacy

Whether developed by governments or tech companies, contact tracing applications can potentially expose user data and violate their right to privacy. If not limited to the minimum required data, these apps can become a surveillance tool. Governments have been developing location-based contact tracing apps as this method offers epidemiologically more useful data. Yet, location data is also more vulnerable to malicious use for political and economic purposes.

Bluetooth-based contact tracing is arguably the most privacy-friendly method. Even if data is centrally stored by public authorities or private firms, it will not include sensitive identity or location data. Of course, no app will perfectly safeguard users' privacy.

Regarding data storage, the most privacy-preserving option would be a decentralized and anonymized contact tracing application. With a decentralized app, collected data are stored in the user devices and are only accessed if an individual is infected. In contrast, as argued by its proponents, the main advantage of a centralized data storage model is that it offers public authorities a greater room of maneuver during the crisis[38].

While most East Asian countries have opted for centralized models, it is highly doubtful that such apps would be widely used under European and North American privacy norms. For instance, in Europe, personal data protection and the right to privacy are highly cherished principles, sensitive to the public as the German contact tracing app debate demonstrated[39].

To set a standard, the European Commission recommended a balanced approach and sensible solution regarding these contact tracing applications[40]. It recommended that the apps must be in full compliance with the rules set forth under data protection and privacy laws. Additionally, it stated that (i) the usage of these apps should not be mandatory for the users and should include sunset provision, (ii) the collected data should not be stored centralized databases, and (iii) the collected data should be anonymized. This approach is in line with Google and Apple's stated intentions.

The centralized solutions might be justifiable now but after the pandemic they will fall under the scope of surveillance. To set a sunset clause might offer some guarantees that the app and the collected data will be deleted after the pandemic. However, more questions arise as to whom will be responsible to decide that the sanitary crisis is over.

37 Covid-Watch, Whitepaper, retrieved May 20, 2020, from https://www.covid-watch.org/article#contactTracing

38 Levy, I. The security behind the NHS contact tracing app, National Cyber Security Center, retrieved May 22, 2020, from https://www.ncsc.gov.uk/blog-post/security-behind-nhs-contact-tracing-app

39 Kelion, L. Coronavirus: German contact-tracing app takes different path to NHS, BBC, retrieved on May 21, 2020, from https://www.bbc.com/news/technology-52650576

40 European Commission, COMMISSION RECOMMENDATION of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data, retrieved May 20, 2020, from https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf

VI. Conclusion

As with any policy solutions, governments' development of contact tracing applications demands a proportionality test. This paper argued this test should be based on the effectiveness of the solution and its privacy guarantees.

One of the main outcomes of this analysis is that regardless of the type of app, it must be used by a sufficient portion of the population to contain the pandemic. To reach a meaningful number, the app needs to inspire trust and usefulness to its users. Trust towards public intervention has no universal standard. While citizens of country A might be more accustomed to invasive public policies, citizens of country B might not welcome such interventions. Thus, culture will play a significant role in the making and use of contact tracing applications.

This paper suggests that especially in democratic societies a Bluetooth-based decentralized contact tracing application has a greater potential to reach the required number of users. By minimizing the range of collected data and limiting government access, this model would respond to most privacy concerns. Of course, this model has also its own setbacks. Firstly, there are security issues inherent with Bluetooth technology. Secondly, it limits the health authorities' room to access and process data which might be useful to contain the pandemic. However, this model is the most suited one to recognize complex contact and offers the most privacy-friendly solution. All-in-all, it has higher probabilities to earn the trust of citizens and reach a meaningful number of users.

The debate surrounding contact tracing apps are first-and-foremost about the equilibrium between safety and privacy. However, underneath this primary discussion, this topic is yet another chapter in the competition over public trust between public authorities and big tech companies. The fact that the public has largely welcomed the Apple/Google API-based model instead of their governments' software must be further researched.

Annex - COVID-19 Contact Tracing Applications Launched or To Be Launched (TBL)

Country	Contact Tracing Application*	Type of Application**	Downloads***
Australia	COVIDSafe	Decentralized Bluetooth	1 000 000
Austria	Stopp Corona	Decentralized Bluetooth	100 000
Bahrain	BeAware	Centralized GPS/location	100 000
Bulgaria	ViruSafe	Centralized GPS/location	10 000
Canada-Alberta[41]	ABTraceTogether	Decentralized Bluetooth	50 000
China	Through WeChat & Alipay apps	Centralized GPS/location	1 164 800 000****
Colombia	CoronaApp	Decentralized Bluetooth	5 000 000
Cyprus	CovTracer	Centralized GPS/location	500
Czechia	ERouska	Decentralized Bluetooth	100 000
Estonia	Estonian Contact Tracing App	Decentralized Bluetooth	TBL
Finland	Ketju	Decentralized Bluetooth	TBL
France	StopCovid	Centralized Bluetooth	TBL
Germany	Corona-Warn-App	Decentralized Bluetooth	TBL
Ghana	GHCOVID-19 Tracker	Centralized GPS/location	Unknown
Hungary	VirusRadar	Decentralized Bluetooth	10 000
Iceland	Rakning C-19	Centralized GPS/location	50 000
India	Aarogya Setu	Centralized GPS/location	100 000 000
Indonesia	PeduliLindungi	Decentralized Bluetooth	1 000 000
Ireland	HSE COVID-19 App	Decentralized Bluetooth	TBL
Israel	HaMagen	Decentralized GPS/location	1 000 000
Italy	Immuni	Decentralized Bluetooth	TBL
Malaysia-1	MyTrace	Decentralized Bluetooth	100 000
Mexico	CovidRadar	Centralized Bluetooth	10 000
Morocco	Wiqaytna	Decentralized Bluetooth	TBL
North Macedonia	StopKorona	Centralized Bluetooth	50 000
Norway	Smittestopp	Centralized Bluetooth	100 000
Poland	ProteGO	Decentralized Bluetooth	10 000
Qatar	Ehteraz	Centralized GPS/location	1 000 000
Singapore	TraceTogether	Centralized Bluetooth	500 000
South Africa	COVI-ID	Centralized GPS/location	100
South Korea	Corona 100m	Centralized GPS/location	1 000 000
Switzerland	SwissCovid	Decentralized Bluetooth	TBL
Tunisia	E7mi	Centralized Bluetooth	10 000
Turkey	Hayat Eve Sığar	Centralized GPS/location	5 000 000
UAE	Trace Covid	Decentralized Bluetooth	100 000
United Kingdom	NHSX	Centralized Bluetooth	TBL
US-Utah	Health Together	Centralized GPS/location	10 000
US-South/North Dakota[42]	Care19	Centralized GPS/location	10 000

* Most of the applications also have other functionalities such as COVID-related information notifications or self-diagnosis.
** This is a simplified classification. Several GPS/location-based applications also use Bluetooth data.
*** These numbers are approximative as only Google Play download records are accessible through open-source data. Yet, the number of Google Play-based downloads are very close to the numbers from public declarations.
**** This data represents the total number of monthly active WeChat users in 2019.

41 The Canadian Government is looking to develop on single application for the whole country: https://www.cbc.ca/news/politics/trudeau-app-contact-tracing-1.5580184

42 Officials from North Dakota are planning to develop a second app compatible with the decentralized Bluetooth API of Apple and Google: https://www.nbcnews.com/tech/tech-news/contact-tracing-apps-are-slow-start-u-s-n1210191

43 Tencent Holding Limited, 2019 Annual Report, retrieved May 22, 2020, from https://cdc-tencent-com-1258344706.image.myqcloud.com/uploads/2020/04/02/ed18b0a8465d8bb733e338a1abe76b73.pdf

Centre for Economics and Foreign Policy Studies

Cyber Governance and Digital Democracy 2020/05/EN

June 2020

SAFETY AND PRIVACY IN THE TIME OF COVID-19: CONTACT TRACING APPLICATIONS

Emre Kursat Kaya | Research Fellow