electronics

MDPI

Article

Digital Contact Tracing: Large-Scale Geolocation Data as an Alternative to Bluetooth-Based Apps Failure

José González-Cabañas [1], Ángel Cuevas [1,2,*], Rubén Cuevas [1,2] and Martin Maier [3]

[1] Department of Telematic Engineering, Universidad Carlos III de Madrid, 28911 Leganés, Spain; jgcabana@it.uc3m.es (J.G.-C.); rcuevas@it.uc3m.es (R.C.)
[2] UC3M-Santander Big Data Institute, 28903 Getafe, Spain
[3] Institut National de la Recherche Scientifique, Montréal, QC H5A 1K6, Canada; martin.maier@inrs.ca
* Correspondence: acrumin@it.uc3m.es

Abstract: The currently deployed contact-tracing mobile apps have failed as an efficient solution in the context of the COVID-19 pandemic. None of them have managed to attract the number of active users required to achieve efficient operation. This urges the research community to re-open the debate and explore new avenues to lead to efficient contact-tracing solutions. In this paper, we contribute to this debate with an alternative contact-tracing solution that leverages the already available geolocation information owned by BigTech companies that have large penetration rates in most of the countries adopting contact-tracing mobile apps. Our solution provides sufficient privacy guarantees to protect the identity of infected users as well as to preclude Health Authorities from obtaining the contact graph from individuals.

Keywords: COVID-19; contact tracing; Facebook; Google; geolocation; privacy

check for updates

Citation: González-Cabañas, J.; Cuevas, Á.; Cuevas, R.; Maier, M. Digital Contact Tracing: Large-Scale Geolocation Data as an Alternative to Bluetooth-Based Apps Failure. *Electronics* **2021**, *10*, 1093. https://doi.org/10.3390/electronics10091093

Academic Editors: Enrique Hernández-Orallo and José M. Cecilia

Received: 20 April 2021
Accepted: 1 May 2021
Published: 5 May 2021

1. Introduction

There is growing evidence that any strategy to effectively fight COVID-19 requires the efficient tracing of all contacts of infected individuals. Recent studies concluded that manual tracing was not sufficiently fast and recommended the use of digital contact tracing systems able to use large-scale location information [1]. A key element of the success of a digital contact-tracing system is its adoption, i.e., the portion of people actively and effectively using that particular system.

Singapore was one of the first countries to implement a digital contact-tracing system in early 2020. They opted to implement a mobile app that used Bluetooth (BT) technology to identify when two users have been in close proximity. If one of those users is tested positive for COVID-19, the other one is identified as a potential contagion. 20% of the population in Singapore installed the mobile app. However, this was not sufficient. Indeed, a representative at the Ministry of Health of Singapore stated that they would need three-quarters of the citizens installing the app to make the digital contact-tracing strategy successful [2].

Although it is not clear what is the adoption rate from which a BT contact-tracing app becomes efficient in controlling a pandemic, some preliminary studies suggest that to mitigate the pandemic an adoption by 60% of the population in a country would be required [1,3]. Some simulation studies showed that if the adoption was below 20% the benefit of a BT contact-tracing app was very small; however, a significant impact was observed with a 40%+ adoption rate [3]. Again, we refer to the rate of people effectively using the app, rather than the number of installations.

BT-based contact-tracing apps have a major problem. They are newly released, and thus they need to achieve the required high adoption rate in a short period of time from scratch. To the best of our knowledge, neither researchers nor public or private institutions have proposed a convincing strategy to achieve the required adoption rate. For the time being, it appears that the success of any BT contact-tracing app depends solely on the self-responsibility of people, and this has not been sufficient.

Despite the described problems and the reported failure of Singapore's app, most western countries (especially in Europe) also opted for mobile apps using BT technology as their contact-tracing systems. In particular, most of these countries opted for using the Decentralized Privacy-Preserving Proximity Tracing (DP-3T) protocol [4]. The main design goal of DP-3T is to provide full-privacy guarantees. In particular, it aims at guaranteeing that the contact-tracing applications using this protocol cannot be misused in the future for privacy-intrusive practices, such as advertising or even massive surveillance. While the authors of this paper agree that the DP-3T protocol provides very strong privacy guarantees, other researchers have exposed that the solution does not provide full-privacy guarantees [5].

To support Health Authorities tat are willing to deploy contact-tracing apps, Google and Apple developed the so-called Google-Apple Exposure Notification (GAEN) system [6] inspired by the DP-3T protocol. GAEN has been integrated into the iOS and Android operating systems. The Operative System (OS) records user encounters using BT and offers this information to the mobile app, which implements the algorithm to identify risk contacts. In spite of this effort, to the best of our knowledge, none of the existing contact-tracing apps has significantly contributed to mitigating the virus transmission thus far.

For instance, early data from the Swiss Health Authority indicates that just 12% of infected individuals reported that they were positive through the app [7]. In Spain, this number shrinks to roughly 2% in practice, despite a recent paper based on a pilot study ran in La Gomera (Canary Island) that raised much higher expectations regarding the efficiency of the app [8]. Finally, a recent report regarding the UK app (England and Wales) [9] presented quite positive results regarding the contribution of the app.

However, in reading the report in detail, we found the results quite disappointing. Although the report states that the number of active users ranged between 24.2% and 33.2%, it does not discuss why the number of active users has largely reduced from 16.5 M to 13 M during December 2020 and January 2021, which implies 21% active users. This is actually an important issue because in the middle of one of the worst periods in the pandemic in the UK the number of active users declined almost 20%. This may reflect the dissatisfaction of users with the app.

The report shows the opacity of this type of solution to provide useful data to HAs. Authors have to rely on models to estimate different metrics to analyze the efficiency of the app. Once more, the results are disappointing. For instance, the authors stated *"Our analysis suggests a relatively large number of COVID-19 cases were averted by contact tracing via the NHS app, ranging from approximately 200,000 to 900,000 depending on the details of the method, compared to the 1.9 million cases that actually arose"*. The large variance reported clearly indicates that it is not feasible to accurately assess the efficiency of fully privacy-preserving apps.

In addition, scientific evidence highlights that the airborne transmission of COVID-19 is irrefutable [10–12], another important limitation of existing BT contact-tracing apps. They are designed to identify short-distance contact between two individuals, i.e., less than 2 m apart. However, airborne transmission implies that contagion between two persons at longer distances is possible. Hence, existing BT contact-tracing apps may miss an important fraction of contacts that should be identified as risk contacts.

Finally, solutions like DP-3T that are designed with the main goal of offering full-privacy present further important shortcomings in the fight against a pandemic. These include: (1) Even if the adoption rate were high, most of the deployed apps require infected users to voluntarily declare their positive condition through the app (excepting very few cases like the Italian app), leaving a very important task such as the control of a pandemic in the hands of individuals' decision. For instance, an early study in Switzerland demonstrates that 1/3 of the users of the app who tested positive did not use the app to report their case [7].

(2) The performance and efficiency of the contact-tracing app cannot be assessed, not even how many infected users have been detected through the app, as recognized by authors of the DP-3T protocol [7]; (3) They are unable to provide aggregate (and not privacy invasive) context information, which might be of great value to improve our knowledge concerning COVID-19 (or other viruses) transmission patterns. For instance, in this paper, we consider the following: revealing aggregate statistics of the type of locations (restaurants, sports facilities, public transportation, hospitals, etc.) infected users visited while they were contagious may be useful to identify statistical biases on the specific type of locations that may reveal hotspots for the virus transmission.

Given the described context, the main goal of this paper is to urge the research community to expand the definition of digital contact-tracing systems having in mind the following key elements: (1) avoid solutions that require massive adoption from scratch as experience has shown; (2) contact-tracing solutions must be designed to consider airborne transmission distance greater than two meters as a reference; (3) guide the design of the solutions setting the *efficiency* in fighting the pandemic (i.e., saving lives and mitigating the impact on the economy) as the primary goal instead of *privacy*. Of course, the proposed solution should be compliant with the existing data protection and privacy laws in the country where it is deployed.

In this paper, we propose an alternative digital contact-tracing system based on the three previous key elements as fundamental design principles:

1. **High adoption rate:** We propose to use real-time location information from (literally) billions of people around the world that is already available in databases of large BigTech companies like Facebook (FB), Google, Apple, etc. We refer to these players as Location Providers (LPs) in this paper. Some of these LPs, mainly Google and Facebook, have a very large rate of active users, over 50%, in many western countries.
2. **Contact identification in airborne transmission range:** To geolocate users at both outdoor [13] and indoor locations [14] with an accuracy of few meters, these BigTech firms use a combination of techniques that rely on multiple signals including GPS location information, WiFi SSIDs signal's power, cellular network signals, etc.
3. **Legal and Ethical Requirements:** We are interested in performing contact-tracing just for individuals who have tested positive of COVID-19. The identity of infected individuals is sensitive information handled by the Health Authority (HA) of each country, which is also responsible for running the contact-tracing strategy. Therefore, the HA has the identity of infected individuals while the LP has the data to perform the contact-tracing for those individuals. We propose a system that allows running contact-tracing using LPs data on those individuals who tested positive as reported by HAs. Even the most restrictive data protection laws, like the GDPR [15], explicitly provision exceptions in which personal data can be used to monitor epidemics and their spread (see GDPR Article 6 Recital 46 [15]). Sustained on this legal basis an agreement to perform an exchange of data between LPs and HAs might be possible. However, to provide higher privacy guarantees, we propose a simple architecture and communication protocol that enable the exchange of information between an LP and a HA significantly limiting the ability of (1) HAs to obtain the contact graph of an individual and (2) LPs to learn the identity of infected individuals.

There are few incipient works in the literature exposing the failure of the deployed contact-tracing apps and proposing alternative solutions that do not rely on new mobile apps [16–19]. We believe it would be important to run pilots for the more promising ones to measure efficiency. To the best of our knowledge, our work is the first that proposes a privacy-preserving solution to implement contact-tracing leveraging fine-grained geolocation data which is readily available.

We acknowledge that this work is a position paper and we have no evidence of whether our system will solve the contact-tracing problem. However, we believe it is a technically sound alternative worth exploring. Additionally, it serves the main purpose of this paper: to encourage the research community to revisit the design of digital contact-tracing solutions in order to create more effective and efficient future mitigation measures vis-à-vis future waves of COVID-19 and other pandemics.

2. Solution Rationale

We propose a novel contact-tracing solution that uses geolocation data of billions of users to find people that have been in contact with individuals who tested positive. We refer to them as *risk contacts*. The geolocation information is owned by BigTech companies referred to as Location Providers (LPs) in this paper, and the information of users tested positive is owned by Health Authorities (HA).

The core of our solution can be described as follow: HAs send to LPs the IDs of infected users. LPs use the location information they own to find the risk contacts of the received IDs (according to the guidelines provided by epidemiology experts) and send back the list of risk contacts IDs to the HA. Finally, HAs reach out to the risk contacts to inform them about the prevention protocol they have to follow.

Note that for practical purposes, we propose to use the mobile phone number of individuals as user IDs in our solution. LPs know the mobile phone number of a major part of the users using their services, and it is reasonable to assume HAs record the mobile phone of infected users to communicate with them.

Unfortunately, the direct exchange of data in clear between HAs and LPs presents important privacy issues. In particular, LPs should not receive clear IDs of infected individuals and HAs should not be able to link the IDs of risk contacts to their correspondent infected user. Our solution addresses this challenge allowing the performing of the contact-tracing task with strong privacy guarantees. To this end, we define an architecture and a communication protocol that involve in addition to LPs and HAs two more players: an Identity Provider (IDP) and an Independent Third-Party Authority (ITPA).

2.1. Why Using Geolocation Data?

Adoption: The main limitation of contact-tracing based on mobile apps is the need to achieve a high rate of active users. This is a major bottleneck that so far has led every attempt in this line to fail.

Our solution avoids this bottleneck using large-scale geolocation data already available and owned by BigTech companies. To explicitly compare the penetration of BigTechs' data vs. BT mobile apps, Table 1 shows for 18 countries we have found data on the number of installations of contact tracing apps: (1) the penetration rate of smartphones, Android OS [20–22] and the Monthly Active Users (MAU) reported by FB [23]; (2) the penetration rate of BT mobile-app in the number of installations as well as an estimation of its penetration in terms of active users.

The list of sources we have used to report the number of mobile apps installations can be accessed here [9,24–36]. Note that, to the best of our knowledge, Switzerland is the unique country reporting the percentage of active users of its app, 63% as of 21 December 2020 [36]. To have an estimation of the fraction of active users for other countries reporting the number of installations, we apply the Swiss ratio to the total number of installations.

According to our estimation, none of the countries reach a significant adoption rate close to 40% for the contact-tracing mobile apps, and only 5 countries are above 20%. In contrast, Facebook penetration is beyond 50% in all countries but Germany (45.5%). Similarly, the penetration of Android is higher than 40% in all countries but the US (32%) and Switzerland (39%). Note that the Android penetration just represents a lower bound of Google penetration. Google has few other extremely popular apps such as Gmail and Google Maps that are widely used by iOS users.

Accuracy: BigTech companies use sophisticated techniques combining GPS, WiFi and cellular networks signals to geolocate users with high precision both outdoors and indoors [13,14]. Google claims to be able to geolocate users with an accuracy of 1 to 2 m using multilateration algorithms based on the WiFi signal from 3 access points. [14].

Therefore, the high penetration rates and location accuracy of BigTech presents them as a data source that may be sufficient to implement efficient contact-tracing solutions. Recent research that used data from LPs with a much lower penetration compared with FB or Google also backed up this hypothesis [37].

Table 1. Penetration in the percentage of smartphones, Android, Facebook, and contact-tracing app installations and the estimated active users for 18 countries. The population of each country to compute the penetration was obtained from The World Bank: Population, total dataset [38]. * The UK active users for the mobile app corresponds only to England and Wales.

Country	Smartphone	Android	Facebook	BT Mobile Apps	
				Installations	Estimated Active Users
Australia	105	44	71.42	27.6	17.4
Austria	117	78	50.25	9	5.7
Belgium	68	41	65.00	12.2	7.7
Croatia	71	59	50.84	2	1,3
Czech Rep	84	66	53.32	14	8.8
Denmark	115	55	71.03	34.8	21.9
Finland	140	97	59.65	45.3	28.5
France	79	51	58.35	9.5	6
Germany	90	61	45.50	34.5	21.7
Ireland	78	42	65.54	40.5	25.5
Italy	84	62	57.80	21.1	13.3
Latvia	96	69	52.45	9.1	5.7
Netherlands	82	48	63.09	25	15.8
Portugal	104	78	67.47	1	0.6
Spain	90	71	62.05	11.5	7.2
Switzerland	97	39	52.38	33.4	21.1
United Kingdom	85	40	66.64	36.05 *	21.7 *
United States	81	32	69.90	2.5	1.6

2.2. Other Benefits

The proposed solution allows for monitoring performance. Geographical locations can be associated with specific categories referred to as Points of Interest (POIs). For instance, a given location can be mapped to a restaurant, a train station, or a hospital. Our solution exploits this to provide a statistical distribution of the POIs visited by infected users vs. POIs visited by the general population. The comparison of these distributions may help to identify statistical biases in POIs that are regularly visited more by infected users, and which might be infection hotspots.

2.3. Privacy Requirements

On the one hand, privacy experts and Data Protection Authorities (DPAs) have shown concerns regarding the use of geolocation information for digital contact tracing. They argued that this may ease governments through their HAs to implement massive surveillance due to the scalability provided by digital technologies.

Therefore, our solution should limit the ability of HAs to massively infer the contact graph information of individuals using the data received from LPs. It should also provide privacy provisions to allow revealing targeted attacks willing to infer the contact graph of particular individuals.

On the other hand, BigTech companies have the means to infer the identity of infected individuals. They can leverage geolocation data and also other information sources, such as emails, posts in social networks, or queries in search engines that they own. For instance, they can detect a user who visited a testing facility after visiting the website and who then remains at home for a period similar to the mandatory quarantine period.

Therefore, we believe that proposals like ours that leverage BigTech companies' geolocation data do not impose any extra risk to infected users' privacy. Despite this, appropriate privacy guarantees should be provided. In particular, our solution should not provide LPs with explicit information about the identity of infected users. It also should limit the ability of LPs to infer such identities from the information received from HAs.

2.4. Meeting Privacy Requirements

To meet the defined privacy requirements, we leverage the following principles: K-anonymity, basic cryptography, and non-repudiation auditing.

K-anonymity: In our solution, the HA sends a list of user IDs to the LP, and the LP answers with the risk contacts of those user IDs. Leveraging the K-anonymity principles, the HA mixes in its request M IDs from infected users and N real random IDs (i.e., random mobile phone numbers associated with real users) where $M <<< N$. This serves to anonymize the identities of infected users and to hinder the capacity of LPs to easily infer the IDs belonging to infected users. The random IDs used by the HA are provided by the Identity Provider (IDP) to guarantee that they are existing IDs. In our solution, IDPs are represented by mobile network operators.

In addition, the HA must aggregate the IDs into groups. There are two types of groups: *infected groups* exclusively include IDs from infected users and *random groups* include IDs from random users or a mix of random and infected users. The messages from the HA to the LP include K groups from which only L are infected groups, where $L <<< K$. Upon the reception of a request message from the HA, the LP computes the risk contacts of each user ID. After that, it aggregates together in the reply the risk contacts of all user IDs into a single group. This aggregation process relies on the K-anonymity concept to prevent the HA from linking the received risk contact IDs to a specific individual. The larger the size of the groups, the higher the privacy guarantees are.

Cryptography: An honest HA is interested only in the risk contact IDs associated with infected groups. To hinder the ability of HAs to access contact IDs from random groups, the LP encrypts the list of contacts of each group (included in the reply to the HA) using a different key per group. Therefore, the HA receives the contact IDs of all groups encrypted. To retrieve the keys of the infected groups, the HA has to send a request to an intermediary that we refer to as Independent Third-Party Authority (ITPA).

In this request, the HA indicates the total number of groups in the query as well as the ID of infected groups. In turn, the ITPA requests the keys of all groups from the LP and forwards to the HA only the keys associated with the infected groups. Finally, using the received keys, the HA obtains the risk contact IDs associated only with the infected groups, thus, completing the contact tracing procedure.

Non-repudiation auditing: Our solution relies on the concept of liability to guarantee the privacy rights of the users. This is a widely adopted approach in the legal system of advanced democracies. For instance, a state cannot prevent anyone from driving above the speed limit, but anyone doing so is liable for it. In the case of privacy, a state cannot prevent a BigTech company from implementing privacy-intrusive practices but can punish them in case where an auditing process reveals the use of those practices. Therefore, a HA or an LP that uses the data they receive for purposes different than contact-tracing will be liable for it.

For instance, a malicious HA can implement a targeted attack (see Section 4) to unveil the contact graph of an individual and leak it to other government branches. This would be a crime equivalent to leaking the medical record of a target individual to other government branches. Our solution collects the required non-repudiation proofs to be used by the corresponding auditing entity to unveil any potential attack by a HA.

3. Protocol for Contact-Tracing Using Location Providers Information

In this section, we describe the steps of the communication protocol (Figure 1), including the sequence of messages exchanged by the four players involved in our solution: the Health Authority (HA), Location Provider (LP), Identity Provider (IDP), and an Independent Third Party Authority (ITPA).

- **Step 0**: This step refers to the basic context that our solution relies on. On the one hand, LPs record historical location information from users running their OSs, mobile apps, etc. They also store the mobile phone number for a major portion of the users. On the other hand, IDPs (i.e., mobile operators) provide users with mobile phone numbers that serve as user IDs in our solution.
- **Step 1**: The HA obtains the IDs of users that have been tested positive in a given time window (e.g., a day).
- **Step 2**: The HA triggers the contact-tracing process by requesting the IDP a list of N user IDs (i.e., real mobile phone numbers). The value of N is decided by the HA and may differ from one request to another.

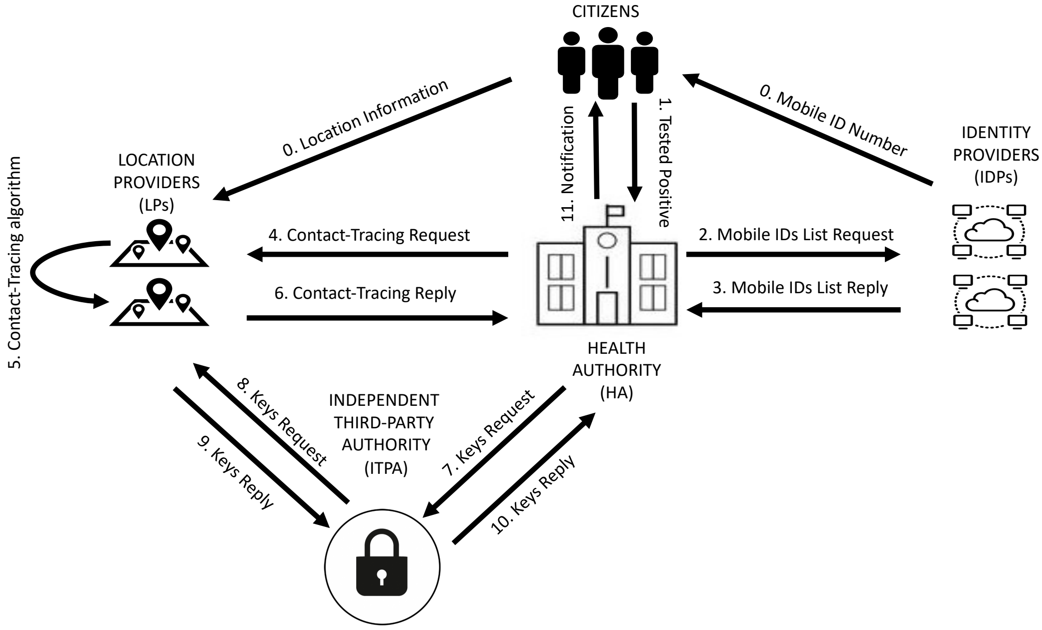

Figure 1. The proposed contact-tracing protocol and architecture.

There are a few remarks to consider: (1) This message includes a unique identifier referred to as the *Transaction ID* that will be included in all the remaining messages in the process. (2) The message is signed with the private key of the HA. During the rest of the process, all entities will sign the messages they send with their private key.

- **Step 3**: The IDP responds to the HA request with a list of N random user IDs.
- **Step 4**: The HA creates K groups. As explained above, only L of these groups are infected groups and $K - L$ are random groups. The resulting groups are included in a *Contact-Tracing Request* message that is sent to the LP. It is important to note that the user IDs included in an infected group can neither be present in other infected groups in this request nor in past or future requests.
- **Step 5**: Upon the reception of the *Contact-Tracing Request*, the LP runs the contact-tracing algorithm to identify the risk contact IDs of each user ID included in the request. The risk contact IDs from all users in a group are aggregated so that any link between a user ID and a risk contact ID is eliminated.

In addition, the LP collects the POIs visited by each user ID in a defined time window in the past (e.g., the last 10 days). Then, the LP computes the distribution of the types of

POIs visited by the user IDs included in each group as well as the overall distribution of the types of POIs visited by all user IDs included in the request.

The information associated with each group, i.e., a list of risk contact IDs and distribution of type of POIs is encrypted with an independent key per group.

Finally, the LP aggregates the encrypted information per group along with the distribution of the types of POIs for all users' IDs and creates a *Contact-Tracing Reply* message that is sent to the HA.

Three important remarks to consider are: (1) The LP must keep a record of the key used to encrypt each group. (2) The contact tracing algorithm implemented by the LP as well as the number of days for the identification of visited POIs must be defined by epidemiologists, and this is out of the scope of this paper. (3) the LP stores all the *Contact-Tracing Request* messages received for auditing purposes.

- **Step 6:** Upon the reception of the *Contact-Tracing Reply* the HA needs to decrypt the information associated with the infected groups, i.e., the risk contacts list and the type of POIs distribution. To this end, the HA sends a *Keys Request* message to the ITPA that includes the total number of groups included in the *Contact-Tracing Request* and the identifiers of the infected groups.
- **Step 7:** The ITPA sends the *Keys Request* message to the LP but includes only the *Transaction ID*.
- **Step 8:** Upon the reception of the *Keys Request* message, the LP sends a *Keys Reply* message to the ITPA that includes the keys for all groups.
- **Step 9:** The ITPA checks if the number of keys in the received reply matches the actual number of groups reported by the HA. If the numbers are the same, the ITPA generates a *Keys Reply* message to the HA that includes only the keys of the infected groups. Otherwise, the *Keys Reply* message includes an error indicating that the reported number of groups does not match with the number of keys provided by the LP.
- **Step 10:** Upon the reception of the *Keys Reply* message, the HA decrypts the information about the risk contacts and the types of POIs distributions included in the *Contact-Tracing Reply* for the groups of infected users.
- **Step 11:** The HA initiates contact with the risk contacts.

4. Potential Attacks and Countermeasures

As explained above, our solution is designed to hinder both the LPs and HAs from misbehaving from having access to information that they are not authorized to obtain. In the following, we explain in detail the countermeasures provided by our solution to avoid: (i) LPs trying to infer the IDs associated with infected individuals, and (ii) HAs trying to obtain the contact graph of citizens.

4.1. LP Inference Regarding an Infected User's Identity

A malicious LP may intend to unveil the identity of infected users based on the information received in *Contact-Tracing Request* messages (known as a re-identification attack). To this end, they could use a single request or combine subsequent requests to obtain the identity of infected users.

To prevent re-identification attacks, the HA has to reuse the IDs that have been already used by including them in random groups of subsequent requests. Otherwise, if random IDs are only used once and discarded, the LP could infer with a very high probability that repeated IDs in different queries belong to infected individuals.

In addition to reusing IDs, our solution relies on the K-anonymity principle. The number of random IDs, N, in the request messages is several times larger than the number of infected user IDs, M. The complexity to perform a re-identification attack grows with the ratio $\frac{N}{M}$.

Our solution allows introducing a high level of randomness into the request messages to avoid LPs being able to infer patterns that allow identifying groups of infected user IDs: (i) the number of infected and random user IDs differs from message to message, (ii) the number of groups in a message differs from message to message, and (iii) the length of the different groups within the same message should also differ. The HA could send messages that do not include any infected user ID from time to time.

Beyond the technical measures, the main argument to support our solution is that powerful LPs, such as Google or Facebook, who are willing to identify infected citizens can easily do this already with the information they own. Therefore, the privacy measures adopted in our solution provide sufficient guarantees to avoid increasing the risk of a potential re-identification attack by LPs.

4.2. HAs Inference Regarding the Contact Graph of a User-ID

Our solution cannot prevent a malicious HA from obtaining the contact graph of a particular individual. For instance, a HA can perform a targeted attack by using the same ID twice in two different infected groups (despite it being forbidden in our solution). The common risk contacts in the two groups may reveal the contact graph of the targeted individual.

However, our solution keeps the required non-repudiation proofs to show that such an attack has happened. The auditing entity simply needs to check whether the HA has used the same ID twice (or more times) in groups of infected users in the same or different messages. The auditing entity can retrieve all the *Contact-Tracing Request* messages from the LP. Similarly, the auditing entity retrieves from the ITPA, for each *Contact-Tracing Request* message, the infected groups declared by the HA. With that information, the auditing entity can easily identify attacks from the HA. The described auditing capacity provides privacy guarantees based on undeniable liability—a widely used technique in developed democracies.

Finally, our recommendation is to run the described auditing process once a day to detect any malicious HA soon after it has implemented an attack.

5. Conclusions

The only digital contact-tracing approach used so far to fight the COVID-19 pandemic consists of the utilization of mobile apps that leverage Bluetooth technology to identify proximity encounters. In this paper, we highlighted the main limitation of this approach—the lack of the sufficient adoption of such mobile apps, which has led every single attempt in this direction thus far to fail.

Due to the importance that digital contact-tracing solutions may have to help to fight pandemics, it is the obligation of researchers, public health authorities, and technology companies to explore alternatives until an effective contact-tracing solution is found. To trigger this exploration effort, in this paper, we propose a promising alternative solution for contact-tracing that invites Health Authorities and BigTech companies to cooperate together.

We propose to use already existing scalable and accurate geolocation data, which is likely to serve to build an efficient digital contact-tracing solution. The presented alternative to the current existing contact-tracing apps relies on the high adoption rate already available from the real-time location information coming from billions of citizens worldwide. This information is stored in datasets of large BigTech companies that already have a large portion of active users. This solution accounts for indoor and outdoor locations, subsequently tackling the demonstrated airborne transmission of COVID-19. Finally, our proposal defines an architecture that leverages such data and provides sufficient privacy guarantees to citizens.

Author Contributions: J.G.-C., Á.C., R.C. and M.M. participated in the conception of the idea; Á.C., R.C., and J.G.-C. defined the solution; Á.C., R.C., and J.G.-C. performed the privacy and security risk analysis. All authors wrote the article. All authors revised the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: The research leading to these results received funding from the European Union's Horizon 2020 innovation action programme under the grant agreement No 871370 (PIMCITY project); the Ministerio de Economía, Industria y Competitividad, Spain, and the European Social Fund(EU), under the Ramón y Cajal programme (Grant RyC-2015-17732); the Ministerio de Educación, Cultura y Deporte, Spain, through the FPU programme (Grant FPU16/05852); the Ministerio de Ciencia e Innovación under the project ACHILLES (Grant PID2019-104207RB-I00); the Community of Madrid synergic project EMPATIA-CM (Grant Y2018/TCS-5046); and the Fundación BBVA under the project AERIS; and the NSERC Discovery Grant 2016-04521.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ferretti, L.; Wymant, C.; Kendall, M.; Zhao, L.; Nurtay, A.; Abeler-Dörner, L.; Parker, M.; Bonsall, D.; Fraser, C. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science* **2020**, *368*. [CrossRef] [PubMed]
2. StraitTimes. Call for More People to Use Contact-Tracing App. 2020. Available online: https://www.straitstimes.com/singapore/call-for-more-people-to-use-contact-tracing-app (accessed on 20 April 2020).
3. Hinch, R.; Probert, W.; Nurtay, A.; Kendall, M.; Wymant, C.; Hall, M.; Lythgoe, K.; Cruz, A.B.; Zhao, L.; Fraser, C.; et al. Effective Configurations of a Digital Contact Tracing App: A Report to NHSX. GitHub. 2020. Available online: https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/Report (accessed on 26 February 2021).
4. Troncoso, C.; Payer, M.; Hubaux, J.; Salathé, M.; Larus, J.; Bugnion, E.; Lueks, W.; Stadler, T.; Pyrgelis, A.; Antonioli, D.; et al. Decentralized Privacy-Preserving Proximity Tracing. *arXiv* **2020**, arXiv:2005.12273.
5. White, L.; van Basshuysen, P. Without a trace: Why did corona apps fail? *J. Med. Ethics* **2021**. [CrossRef] [PubMed]
6. Apple; Google. Exposure Notifications: Using Technology to Help Public Health Authorities Fight COVID-19. 2021. Available online: https://www.google.com/covid19/exposurenotifications/ (accessed on 26 February 2021).
7. Salathé, M.; Althaus, C.L.; Anderegg, N.; Antonioli, D.; Ballouz, T.; Bugnion, E.; Čapkun, S.; Jackson, D.; Kim, S.I.; Larus, J.R.; et al. Early Evidence of Effectiveness of Digital Contact Tracing for SARS-CoV-2 in Switzerland. *medRxiv* **2020**. [CrossRef]
8. Rodríguez, P.; Graña, S.; Alvarez-León, E.E.; Battaglini, M.; Darias, F.J.; Hernán, M.A.; López, R.; Llaneza, P.; Martín, M.C.; Ramirez-Rubio, O.; et al. A population-based controlled experiment assessing the epidemiological impact of digital contact tracing. *Nat. Commun.* **2021**, *12*, 1–6. [CrossRef] [PubMed]
9. Wymant, C.; Ferretti, L.; Tsallis, D.; Charalambides, M.; Abeler-Dörner, L.; Bonsall, D.; Hinch, R.; Kendall, M.; Milsom, L.; Ayres, M.; et al. *The Epidemiological Impact of the NHS COVID-19 App*; Alan Turing Institute: London, UK, 2021. Available online: https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/Epidemiological_Impact_of_the_NHS_COVID_19_App_Public_Release_V1.pdf (accessed on 26 February 2021).
10. Scientific Brief: SARS-CoV-2 and Potential Airborne Transmission. Centers for Disease Control and Prevention (CDC). 2020. Available online: https://www.cdc.gov/coronavirus/2019-ncov/more/scientific-brief-sars-cov-2.html (accessed on 27 December 2020).
11. Prather, K.A.; Marr, L.C.; Schooley, R.T.; McDiarmid, M.A.; Wilson, M.E.; Milton, D.K. Airborne transmission of SARS-CoV-2. *Science* **2020**, *370*, 303–304. [CrossRef] [PubMed]
12. Lednicky, J.A.; Lauzardo, M.; Fan, Z.H.; Jutla, A.; Tilly, T.B.; Gangwar, M.; Usmani, M.; Shankar, S.N.; Mohamed, K.; Eiguren-Fernandez, A.; et al. Viable SARS-CoV-2 in the air of a hospital room with COVID-19 patients. *medRxiv* **2020**. [CrossRef]
13. GPS.gov. GPS Accuracy. 2017. Available online: https://www.gps.gov/systems/gps/performance/accuracy/ (accessed on 20 April 2020).
14. Google. Wi-Fi Location: Ranging with RTT. 2020. Available online: https://developer.android.com/guide/topics/connectivity/wifi-rtt (accessed on 20 April 2020).
15. European Union. Regulation (EU) 2016/679 of the European Parliament (General Data Protection Regulation). 2016. Available online: http://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 22 April 2020).
16. Mokbel, M.; Abbar, S.; Stanojevic, R. Contact Tracing: Beyond the Apps. *SIGSPATIAL Spec.* **2020**, *12*, 15–24. [CrossRef]
17. Reichert, L.; Brack, S.; Scheuermann, B. Privacy-Preserving contact tracing of COVID-19 patients. *IACR Cryptol. ePrint Arch.* **2020**, *2020*, 375.
18. Nakamoto, I.; Wang, S.; Guo, Y.; Zhuang, W. A QR Code–Based Contact Tracing Framework for Sustainable Containment of COVID-19: Evaluation of an Approach to Assist the Return to Normal Activity. *JMIR mHealth uHealth* **2020**, *8*, e22321. [CrossRef] [PubMed]
19. Rahman, M.T.; Khan, R.T.; Khandaker, M.R.; Sellathurai, M.; Salan, M.S.A. An automated contact tracing approach for controlling COVID-19 spread based on geolocation data from mobile cellular networks. *IEEE Access* **2020**, *8*, 213554–213565. [CrossRef]
20. Dimoco. Market Insights. 2020. Available online: https://dimoco.eu/carrierbilling/coverage/ (accessed on 27 December 2020).
21. StatCounter Global Stats. Mobile Operating System Market Share Worldwide. 2020. Available online: https://gs.statcounter.com/os-market-share/mobile/ (accessed on 27 December 2020).
22. Demographics of Mobile Device Ownership and Adoption in the United States. 2020. Available online: https://www.pewresearch.org/internet/fact-sheet/mobile/ (accessed on 27 December 2020).

23. Facebook. Facebook Marketing API. 2020. Available online: https://developers.facebook.com/docs/marketing-apis (accessed on 27 December 2020).
24. Austria: The Official Travel Portal. Austria's "Stopp Corona" app helps your peace of mind on holiday. 2020. Available online: https://www.austria.info/en/service-and-facts/coronavirus-information/app (accessed on 27 December 2020).
25. Australian Government. COVIDSafe App. 2020. Available online: https://www.covidsafe.gov.au/ (accessed on 27 December 2020).
26. COSIC—ESAT KU Leuven. Coronalert: A Promising Start. 2020. Available online: https://www.esat.kuleuven.be/cosic/blog/coronalert-a-promising-start/ (accessed on 20 October 2020).
27. Government of the Republic of Croatia. Stop COVID-19. 2020. Available online: https://www.koronavirus.hr/stop-covid-19-723/723 (accessed on 27 December 2020).
28. eRouška. Frequently Asked Questions. 2020. Available online: https://erouska.cz/caste-dotazy#statistiky (accessed on 27 December 2020).
29. Smitte | stop. Driftsstatus. 2020. Available online: https://smittestop.dk/status/ (accessed on 27 December 2020).
30. Finnish Institute for Health and Welfare. Koronavilkku Has Been Downloaded More than 2.5 Million Times—Widespread Use Increases the App's Effectiveness. 2020. Available online: https://thl.fi/en/web/thlfi-en/-/koronavilkku-has-been-downloaded-more-than-2.5-million-times-widespread-use-increases-the-app-s-effectiveness (accessed on 5 November 2020).
31. Latvian Public Broadcasting. "Stop COVID" App Has Helped 110 Times Already in Latvia. 2020. Available online: https://eng.lsm.lv/article/society/health/stop-covid-app-has-helped-110-times-already-in-latvia.a379047/ (accessed on 23 October 2020).
32. Overheid.nl Open Data of the Government. Dataset CoronaMelder Statistieken. 2020. Available online: https://data.overheid.nl/en/dataset/coronamelder-statistieken (accessed on 27 December 2020).
33. Pickaso. Infografía: Evolución Apps Móviles de Radar COVID-19 en Europa. 2020. Available online: https://pickaso.com/2020/infografia-apps-radar-covid-europa (accessed on 31 October 2020).
34. Briers, M.; Holmes, C.; Fraser, C. *Demonstrating the Impact of the NHS COVID-19 App*; Alan Turing Institute: London, UK, 2021. Available online: https://www.turing.ac.uk/blog/demonstrating-impact-nhs-covid-19-app (accessed on 26 February 2021).
35. NBC News. Despite Promise, Few in US Adopting COVID-19 Exposure Apps. 2020. Available online: https://www.nbcnews.com/tech/tech-news/promise-us-adopting-covid-19-exposure-apps-rcna189 (accessed on 7 December 2020).
36. Swiss Federal Statistical Office. Swiss Covid App Monitoring. 2020. Available online: https://www.experimental.bfs.admin.ch/expstat/en/home/innovative-methods/swisscovid-app-monitoring.assetdetail.13407769.html (accessed on 27 December 2020).
37. Aleta, A.; Martín-Corral, D.; Bakker, M.A.; Piontti, A.P.Y.; Ajelli, M.; Litvinova, M.; Chinazzi, M.; Dean, N.E.; Halloran, M.E.; Longini, I.M.; et al. Quantifying the importance and location of SARS-CoV-2 transmission events in large metropolitan areas. *medRxiv* **2020**. [CrossRef]
38. The World Bank: Population, Total. 2020. Available online: https://data.worldbank.org/indicator/SP.POP.TOTL (accessed on 27 December 2020).