NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS

SCHOOL OF SCIENCE
DEPARTMENT OF INFORMATICS AND TELECOMMUNICATIONS

POSTGRADUATE PROGRAM
COMPUTER, TELECOMMUNICATIONS AND NETWORK ENGINEERING

THESIS

Security and Privacy of Contact Tracing Applications

Symela – Foteini N. Komini

Supervisor: **Konstantinos Limniotis,** External Instructor

ATHENS

JUNE 2022

ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
"ΜΗΧΑΝΙΚΗ ΥΠΟΛΟΓΙΣΤΩΝ, ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΔΙΚΤΥΩΝ"

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Security and Privacy of Contact Tracing Applications

Συμέλα – Φωτεινή Ν. Κομίνη

Επιβλέπων: **Κωνσταντίνος Λιμνιώτης**, Διδάσκων εκτός Τμήματος

ΑΘΗΝΑ

ΙΟΥΝΙΟΣ 2022

THESIS

Security and Privacy of Contact Tracing Applications

Symela - Foteini N. Komini
A.M.: en3190002

SUPERVISOR: **Konstantinos Limniotis,** External Instructor

EXAMINATION COMMITEE:	**Hadjiefthymiades Stathes,** Professor **Nikos Pasas,** Laboratory Teaching Staff

June 2022

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Security and Privacy of Contact Tracing Applications

Συμέλα - Φωτεινή Ν. Κομίνη
Α.Μ.: en3190002

ΕΠΙΒΛΕΠΩΝ: **Κωνσταντίνος Λιμνιώτης,** Διδάσκων εκτός Τμήματος

ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ: **Ευστάθιος Χατζηευθυμιάδης,** Καθηγητής
Νίκος Πασσάς, Εργαστηριακό Διδακτικό Προσωπικό (ΕΔΙΠ)

Ιούνιος 2022

ABSTRACT

The focus of this thesis is the security and privacy of contact tracing applications. The rules and guidelines provided by European Data Protection Board and General Data Protection Regulation for the development and functionality of contact tracing applications will be presented, as well as, a high-level description of the main architectures and technologies used in contact tracing, the advantages and disadvantages of each, security threats and privacy concerns and examples of their functionality. There is also an analysis concerning developed contact tracing applications around the world over the past 2 years, where the findings and how acceptable and privacy-proof is each application, are discussed. Based on the aforementioned analysis, the trackers and permissions required for each application are investigated and the manner in which these affect the adoption of the application is discussed. Finally, there is our suggestion of the guidelines a Greek contact tracing application should follow to be secure, private and successfully adopted from the public.

SUBJECT AREA: Security and Privacy

KEYWORDS: Contact, Tracing, Application, Security, Privacy

ΠΕΡΙΛΗΨΗ

Αυτή η διατριβή εστιάζει στην ασφάλεια και το απόρρητο των εφαρμογών ανίχνευσης επαφών. Παρουσιάζονται οι κανόνες και οι κατευθυντήριες γραμμές που παρέχονται από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων και τον Γενικό Κανονισμό Προστασίας Δεδομένων για την ανάπτυξη και τη λειτουργικότητα των εφαρμογών ανίχνευσης επαφών. Στη συνέχεια, γίνεται μια περιγραφή υψηλού επιπέδου των κύριων αρχιτεκτονικών και τεχνολογιών που χρησιμοποιούνται στην ανίχνευση επαφών, παρουσιάζονται τα πλεονεκτήματα και τα μειονεκτήματα καθεμιάς, οι απειλές για την ασφάλεια και οι ανησυχίες για το απόρρητο, καθώς και παραδείγματα της λειτουργικότητάς τους. Υπάρχει επίσης μια ανάλυση σχετικά με τις αναπτυγμένες εφαρμογές ανίχνευσης επαφών σε όλο τον κόσμο τα τελευταία 2 χρόνια, όπου συζητούνται τα ευρήματα, το πόσο αποδεκτή είναι καθώς και το πόσο καλά προστατεύει την ιδιωτικότητα η εκάστοτε εφαρμογή. Πάνω σε αυτήν την ανάλυση, γίνεται έρευνα των trackers και των αδειών που απαιτούνται για κάθε εφαρμογή, και συζήτηση για το πώς αυτά επηρεάζουν την υιοθέτηση της εφαρμογής από το κοινό. Τέλος, υπάρχει η πρότασή μας για τις οδηγίες που πρέπει να ακολουθεί μια ελληνική εφαρμογή ανίχνευσης επαφών για να είναι ασφαλής, ιδιωτική και να υιοθετηθεί με επιτυχία από το κοινό.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Ασφάλεια και Ιδιωτικότητα

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Επαφή, Ιχνηλάτηση, Εφαρμογή, Ασφάλεια, Ιδιωτικότητα

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα εργασία αποτελεί διπλωματική εργασία στα πλαίσια του μεταπτυχιακού προγράμματος «Μηχανική Υπολογιστών, Τηλεπικοινωνιών και Δικτύων» με ειδίκευση την «Δικτύωση Υπολογιστών» του τμήματος Πληροφορικής και Τηλεπικοινωνιών του Εθνικού & Καποδιστριακού Πανεπιστημίου Αθηνών. Η ολοκλήρωση της διπλωματικής θα ήταν αδύνατη χωρίς την πολύτιμη υποστήριξη του επιβλέποντος καθηγητή, κ. Λιμνιώτη Κωνσταντίνο. Τον ευχαριστώ θερμά για την εμπιστοσύνη που μου έδειξε για να φέρω εις πέρας μια διπλωματική με ένα τόσο επίκαιρο θέμα, για τις υποδείξεις, την συμπαράσταση και την άμεση επικοινωνία που είχαμε καθ’ όλη τη διάρκεια της εργασίας. Θέλω επίσης να ευχαριστήσω βαθιά το σύντροφό μου για την συνεχή συμπαράσταση, βοήθεια και κατανόηση του όλο αυτό το διάστημα. Τέλος, θα ήθελα να ευχαριστήσω τους γονείς μου, στους οποίους οφείλω όλη τη διαδρομή των σπουδών μου μέχρι σήμερα.

TABLE OF CONTENTS

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

1. INTRODUCTION

Since the beginning of 2020, Covid-19 has turned into a global pandemic challenging both health care systems as well as democratic institutions. The manual tracing of possibly infected people could not keep up with the increasing rate of new infections. As a result, numerous lock-downs have taken place all over the world the last 2 years, challenging the economies. In order to counter the rapid spread of the virus, an automatic tracing tool was created. Those tools are the contact tracing applications. Since contact tracing involves a lot of personal information (e.g. location, encounters), there was the need for privacy preserving guidelines to be established. Thus, the European Data Protection Board has provided a set of rules and guidelines for the development of contact tracing applications, taking into consideration the General Data Protection Regulation rules for the user's privacy.

Following the guidelines of EDPB and GDPR, many applications have been developed worldwide. There are many questions that need to be answered while designing a contact tracing application. First and foremost, what kind of user data are collected. The provided guidelines do mention the minimum necessary data that needs to be collected in order to ensure the privacy of the user, however, some countries do not collect just the minimum as we will see later in the thesis. Then there is the question of where the collected data are stored and, most importantly, who has access to them. There are two architectures designed, a centralized one and a decentralized one. In the first case, data are collected, processed and stored in a server, while in the second case, the data remain and are processed on the user's device. Data stored on user's device are only accessible by the user while the server is accessible from the appointed authority and/or third parties.

Another important part of contact tracing functionality is how the contact tracing takes place. There are different technologies implemented for this purpose, such as Bluetooth, GPS and QR codes. Each one having their own advantages and disadvantages. We will later analyze the two most used contact tracing technologies and do a mini-comparison of them.

The guidelines are to ensure that the development of the application is done correctly, but, it is also important for the public to adopt the applications in order for them to be efficacious. Keeping that in mind, many governments have done public debates about the developing applications, so that there is transparency of the process and the public won't be hesitant once the application is complete and available. Other countries have ignored this need, resulting in smaller rates of adoption. We will later analyze the reasons that affect the public's attitude towards contact tracing applications, as well as general privacy concerns.

This thesis is focused on the privacy and security of contact tracing applications. The issues we will analyze and the questions we will answer are the following:

1. Which are the main features, as well as the relative advantages and disadvantages, for the various types of contact tracing applications?
2. What are the public's privacy concerns?
3. Are contact tracing applications vulnerable to security attacks? If yes, how can we defend against them?
4. After 2 years of COVID-19 crisis, which are the contact tracing applications worldwide? Are they privacy-proof? What are the required permissions and the trackers of each application?

5. If Greece develops a contact tracing application, there is our suggestion as to the guidelines and steps the developers and the government should follow.

2. GENERAL DATA PROTECTION REGULATION

The COVID-19 pandemic has shaken the whole world on many levels. As a response, governments are turning towards the use of data driven solutions in order to limit the pandemic. Such type of solutions, however, tends to raise numerous concerns regarding the users' privacy.

Any solution suggested by the governments should be socially acceptable in order for it to be efficient and effective. To achieve that, data protection is indispensable to build trust. Users must be sure that their personal data will be collected and processed correctly in order to monitor and contain the spread of COVID-19 and not to control, stigmatize or repress individuals.

The European Data Protection Board (EDPB) highlights the flexibility of data protection legal framework, which allows both the limitation of the pandemic and the protection of human rights and freedoms. The General Data Protection Regulation (GDPR) [1] and Directive 2002/58/EC ("ePrivacy Directive") contain specific rules allowing for the use of anonymous or personal data to support public authorities and other actors at national and EU levels in monitoring and containing the spread of the virus [2].

Contact tracing applications are a data driven solution and their purpose is to alert people who are potentially exposed to the virus, in order to break the contamination chains as early as possible.

2.1 Definitions

Here are the basic definitions for contact tracing:

- Personal data is any kind of data about a natural person ("data subject") than can be used to identify the person directly or indirectly.
- Processing refers to the way personal data is handled, whether via automated or manual means.
- Profiling refers to the processing of data analyze or predict aspects about the person's preferences or state of life.
- Pseudonymization is the processing of data in such a way that no data subject can be identified without the use of additional information, which is kept separately.
- The controller is the person or body that determines why and how are personal data supposed to be processed.
- The processor is the person or body that performs processing on the data on behalf of the controller.
- The recipient is the person or body to which the personal data are disclosed. Public authorities shall not be regarded as recipients.
- A third party is any person or body other than the data subject, controller, processor and anyone else authorized by the above to process the data.
- Consent of the data subject is the informed, free and unambiguous indication of the subject's wishes towards the processing of their personal data.
- Genetic, biometric and health concerning data are all different types of personal data, although not exhaustively.

- Main establishment is the place where the actions of either the controller or the processor are occurring.
- Binding corporate rules are the policies adhered to by a controller or processor for transfers of personal data to a controller or processor in one or more third countries.
- A supervisory authority is concerned by the processing of personal data either because the controller or processor is established in its territory, the data subjects residing in its territory are (likely to be) substantially affected by the processing, or a complaint has been lodged with that authority.
- Cross-border processing means either the processing of personal data in more than one Member States, or the processing of personal data which substantially affects of is likely to substantially affect data subjects in more than one Member State.

2.2 Principles for personal data processing

Personal data shall be:

- Processed lawfully, fairly and in a transparent manner. (lawfulness, fairness and transparency)
- Collected for specified, explicit and legitimate purposes only (statistical/historical/scientific purposes are not considered incompatible with this). (purpose limitation)
- Adequate, relevant and limited to what is necessary. (data minimization)
- Accurate and, where necessary, kept up to date. (accuracy)
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes defined. (storage limitation)
- Processed in a manner that ensures appropriate security of the personal data. (integrity and confidentiality)

The controller shall be responsible for, and be able to demonstrate compliance with the above (accountability).

2.3 Lawfulness of processing

Lawful processing demands at least one of the following being met:

1. Data subject has given consent
2. Processing is necessary for a contract to which the data subject is party
3. Processing is necessary for legal obligation compliance
4. Processing is necessary for protecting the data subject’s or other natural person’s vital interests
5. Processing is necessary for task of public interest or in the exercise of official authority vested in the controller
6. Processing is necessary for legitimate interests of the controller or third party, except where such interests are overridden by fundamental rights and freedoms of the data subject

Member States may have more specific terms in place to adapt the application of the above rules by determining more precisely specific requirements for the processing of personal data.

The basis of the processing for points (3) and (5) shall be determined either by Union law or by Member State law to which the controller is subject. The purpose of the processing shall be defined in that legal basis. That basis may contain specific terms to adapt the application of the above rules with regards to:

- the general conditions governing the lawfulness of processing by the controller
- the types of data which are subject to the processing
- the data subjects concerned
- the entities to, and the purposes for which, the personal data may be disclosed
- the purpose limitation
- storage periods
- processing operations and processing procedures, including measures to ensure lawful and fair processing

The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

Where processing of data is not in line with the reasons for which the data were collected and is not based on the data subject’s consent or on Union or Member State law, the controller shall, in order to declare whether processing for another purpose is compatible with the initial purpose, take into account:

- any connection between the initial and further purposes
- the context in which the personal data were collected, regarding the relationship between the controller and the data subjects
- the nature of the personal data, especially considering special categories of data or data related to criminal convictions and offenses
- the possible consequences of the intended further processing of the data
- the existence of appropriate measures, such as encryption or pseudonymization

2.4 How special categories of data must be processed

The processing of personal data that reveal a person’s ethnicity, their political opinions, religious or philosophical beliefs, or trade union membership, along with the processing of genetic data, biometric data in order to uniquely identify a natural person, health related data or data concerning a natural person's sex life or sexual orientation is strictly prohibited.

However, there are a few exemptions to the previous if one (or more) of the following apply:

a) the data subject has explicitly consented to the processing of those personal data for purposes specifically specified, with the exemption of where Union or Member State law provide that the data subject may not lift the prohibition that is referred to in the previous paragraph.

b) processing is necessary to carry out the obligations and to exercise specific rights of the controller or of the data subject in the field of employment and social security and social protection law, as long as it is authorized by Union or Member State law or a collective agreement pursuant to Member State law that provides for appropriate safeguards assuring the fundamental rights and interests of the data subject.

c) processing is needed in order to protect the data subject’s vital interests or the interests of another natural person, in cases where the data subject is not physically or legally capable of giving consent.
d) processing is carried out by a foundation, association or any other non-profit body with a philosophical, political, religious or trade union aim, in the course of its legitimate activities with appropriate safeguards, and only if the processing relates solely to the members or to former members of the body or to persons who have regular contact with it associated with its purposes and that the personal data are disclosed only inside of that body and their disclosure is strictly prohibited without the consent of the data subjects;
e) processing relates to personal data and those data have been manifestly made public by the data subject.
f) processing is necessary in order to establish, exercise or defend legal claims or whenever courts are acting in their judicial capacity.
g) processing is needed in favor of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, in order to respect the essence of the right to data protection and provide for suitable and specific measures aiming to safeguard the fundamental rights and interests of the data subject.
h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the of the employee’s working capacity, medical diagnosis, the provision of health or social care or treatment or for the purposes of managing health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in next paragraph.
i) processing is needed for reasons of public interest in the public health sector, such as protection against serious cross-border health threatening situations or as a way of ensuring high quality and safety standards of health care and of medicinal products, on the basis of Union or Member State law which provides for suitable and specific measures to ensure the rights and freedoms of the data subject, processed with particular professional secrecy.
j) processing is necessary for archive-related purposes in the public interest, science or history-related research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respecting the essence of the right to data protection and providing for suitable and specific measures in order to safeguard the fundamental rights and interests of the data subject.

Personal data referred to in the first paragraph may be processed for the purposes that are mentioned in point (h) of the previous paragraph, when those data are processed by or under the responsibility of a professional who is obliged to behave in professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules which national competent bodies have established. Finally, Member States may maintain or introduce further conditions, such as limitations, regarding the processing of genetic and biometric data, or data concerning health.

2.5 Data protection by design

The controller of the data shall implement appropriate technical and organizational measures, such as pseudonymization, which are designed for the purpose of implementing data-protection principles, such as data minimization, in an effective manner and for integrating the necessary safeguards into the processing aiming to meet the requirements of this Regulation and to protect the rights of data subjects (the controller shall do the above not only at the time of the determination of the means for processing but also at the time of the processing itself).

In order to ensure that, by default, only the personal data necessary for each specific purpose of the processing are processed, the controller should implement appropriate organizational and technical measures. This obligation applies to the extent of the processing of the personal data, the amount of collected, the period of their storage as well as their accessibility. More specifically, the above measures shall ensure that by default personal data are made accessible only with the individual's intervention to an indefinite number of natural persons.

2.6 Security of processing

The processor of the personal data shall take on some appropriate measures of technical and organizational nature in order to ensure a level of security appropriate to the risk, including some of the following:

a) the personal data is encrypted and pseudonymized
b) the processing systems and services are ongoingly operating in a confidential, resilient and with high integrity way
c) the availability and access to the personal data shall be restored in a timely manner in case of technical or physical accident
d) the security of processing is ensured by a process of regular testing, assessment and evaluation of the effectiveness of organizational and technical measures

Moreover, in order to assess the appropriate level of security, one shall give more attention particularly to the risks that are presented by processing, especially from accident-related or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data transmitted, stored or processed in any other way.

All in all, the controller and processor shall act to ensure that any natural person acting under the authority of the controller or the processor, with access to personal data, does not process them except when instructed by the controller, unless they are required to do so by Union or Member State law.

3. THE EUROPEAN DATA PROTECTION BOARD

In regard of users' privacy, the EDPB has already taken position on the fact that the use of contact tracing applications should be voluntary and should not rely on tracing individual movements but rather on proximity information regarding users [3].

Use of location data

According to ePrivacy Directive, 'location data' means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

Sources of location data

Location data can help model the spread of the virus as well as the overall effectiveness of the confinement measures. There are two principal sources of location data:

- location data collected by electronic communication service providers (such as mobile telecommunication operators) in the course of the provision of their service, and
- location data collected by information society service providers' applications whose functionality requires the use of such data (e.g., navigation, transportation services, etc.).

The location data collected from electronic communication providers can be processed within the remits of articles 6 and 9 of the ePrivacy Directive [4]. This means that the service provider must inform the users or subscribers,

- of the type of location data which will be processed,
- of the purposes and duration of the processing and
- whether the data will be transmitted to authorities or third parties.

Regarding location data collected directly from the terminal equipment, art. 5(3) of the "ePrivacy" directive applies [4]. That means that the storing of information on the user's device or gaining access to the information already stored is allowed only if (i) the user has given consent or (ii) the storage and/or access is strictly necessary for the information society service explicitly requested by the user.

What is data anonymization? Data anonymization is the process of destroying tracks, or the electronic trail, on the data that an eavesdropper could use to trace its origins. An electronic trail is the information that is left behind when someone sends data over a network. Forensic experts can follow the data to figure out who sent it. So, if someone has the knowledge and the skills, they can track individuals with specific characteristics, such as being infected, in our case. These scenarios are not acceptable in contact tracing applications, so data anonymization techniques are to be utilized. However, caution is crucial since the process can be reversed! Many current techniques associated with anonymization can be bypassed as there are ways to reveal stripped personally-identifying information (PII) from datasets. One way this information can be revealed is with cross referencing any sets of records still visible. This process is called deanonymizing [5].

A sum of different data anonymization techniques, how they work and how they can be de-identified is displayed in Figure 1 [6]. Both anonymization processes and re-identification attacks are active fields of research, so any controller implementing anonymization solutions must monitor recent developments in this field, especially concerning location data (originating from telecom operators and/or information society services) which are known to be notoriously difficult to anonymize.

It is, also, crucial that anonymized data must pass through a test which takes into account both objective aspects (time, technical means) and contextual elements that may vary case by case (rarity of a phenomenon including population density, nature and volume of data). If the data fails in this test, then it is not considered anonymized and it remains in the scope of GDPR. In this sense, anonymization processes must consider location datasets as a whole and process data from a reasonably large set of individuals using available robust anonymization techniques.

But how can we be sure that the anonymization techniques that we utilize are strong enough? The robustness of the anonymization relies on three criteria [7]:

- singling-out (isolating an individual in a larger group based on the data),
- linkability (linking together two records concerning the same individual) and
- inference (deducing, with significant probability, unknown information about an individual).

Given the complexity of anonymization processes, transparency regarding the anonymization methodology is highly encouraged.

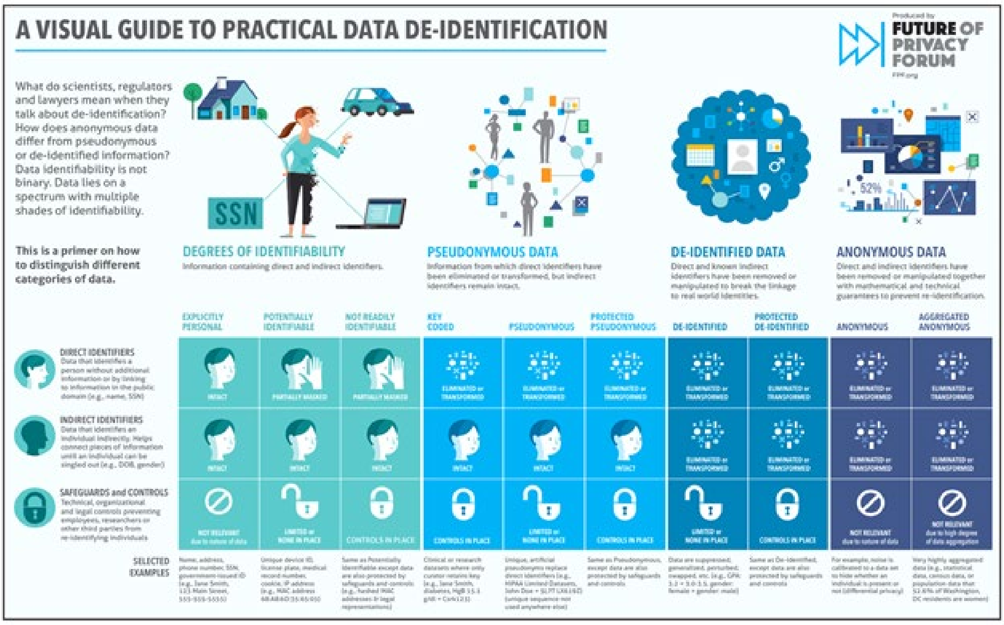
A VISUAL GUIDE TO PRACTICAL DATA DE-IDENTIFICATION
Produced by
FUTURE OF PRIVACY FORUM
FPF.org
What do scientists, regulators and lawyers mean when they talk about de-identification? How does anonymous data differ from pseudonymous or de-identified information? Data identifiability is not binary. Data lies on a spectrum with multiple shades of identifiability.
This is a primer on how to distinguish different categories of data.
SSN
52%
DEGREES OF IDENTIFIABILITY
Information containing direct and indirect identifiers.
PSEUDONYMOUS DATA
Information from which direct identifiers have been eliminated or transformed, but indirect identifiers remain intact.
DE-IDENTIFIED DATA
Direct and known indirect identifiers have been removed or manipulated to break the linkage to real world identities.
ANONYMOUS DATA
Direct and indirect identifiers have been removed or manipulated together with mathematical and technical guarantees to prevent re-identification.
EXPLICITLY PERSONAL
POTENTIALLY IDENTIFIABLE
NOT READILY IDENTIFIABLE
KEY CODED
PSEUDONYMOUS
PROTECTED PSEUDONYMOUS
DE-IDENTIFIED
PROTECTED DE-IDENTIFIED
ANONYMOUS
AGGREGATED ANONYMOUS
DIRECT IDENTIFIERS
INDIRECT IDENTIFIERS
SAFEGUARDS and CONTROLS
INTACT
PARTIALLY MASKED
ELIMINATED or TRANSFORMED
NOT RELEVANT due to nature of data
LIMITED or NONE IN PLACE
CONTROLS IN PLACE
NOT RELEVANT due to high degree of data aggregation
SELECTED EXAMPLES

Figure 1. Different techniques of data anonymization and de-identification

3.1 Contact Tracing Applications

As mentioned before, users must voluntarily use the contact tracing applications, since monitoring their location and/or contacts with other people, is an intrusion to their privacy. For a user to allow such a monitoring, they must trust the application and the process behind it should be transparent to them. But how can we achieve that? EDPB has some guidelines for both of them that provide a general guidance to designers and

Implementers of contact tracing applications.

3.1.1 Legal Analysis

In order to ensure the highest level of transparency of the process:

- The controller of the contact tracing applications must be defined and known to users, in order to ensure accountability. A consideration for that position are the national health authorities, however, other controllers can also be envisaged. If there are different actors involved in contact tracing applications deployment, then their roles and responsibilities must be clearly established and explained to the users.
- The objective of the applications must be clear in order to limit the personal data collected from a user, as well as their processing, to purposes related to COVID-19 health crisis management only.
- The categories of data that are going to be used, should be defined. There should also be safeguards placed in order to avoid re-identification of the individuals. Contact tracing applications may require the collection of health data. The processing of such data is allowed, when necessary, for reasons of public health, for scientific research purposes or statistical purposes, based on article 9(2) of GDPR.
- The information the application has collected, should reside on the user's equipment and only the relevant information should be retrieved when necessary. The fact that the app is used voluntarily does not mean that all user's data can be processed without their consent. A provider must ask the user's permission to access data on their equipment, if that data is not strictly necessary for providing the service requested by the user.
- The criteria that determine when the contact tracing applications should be dismantled as well as which entity will take the responsibility and accountability for making that decision, should be defined. Once the contact tracing applications are dismantled, all personal data should be erased or anonymized.

3.1.2 Application guidelines

Once the users have a clear picture of the process, they must also be sure that the information that contact tracing applications will be collecting, will not be used for purposes other than facing COVID-19 crisis and that they won't be stigmatized in any way while using these applications.

Contact tracing applications should:

- collect only the absolutely necessary data from the user's terminals. Any information unrelated or not needed for the purposes of containing the virus, should not be collected, transmitted or used.
- Any information that allows the users to infer the identity or the diagnosis of others, should not be conveyed by the applications.

- In order to monitor the contacts an individual had with other people, proximity data should be used instead of tracking their location, hence, location data should not be collected or used.
- The operation of these applications is to broadcast and receive data to and from other user's devices, accordingly. The transmitted data includes only unique and pseudonymous identifiers that are generated by the app, using state-of-the-art cryptographic processes, and are specific to it. Such identifiers should be renewed at such a rate that there is no risk of identifying and/or tracking individuals, as well as, keeping pace with the rate the virus is spreading.
- When an application communicates with the server, mutual authentication between them must be performed.
- If a user is diagnosed as infected, the server can collect data regarding the contact history or the identifiers broadcasted by the user’s application, only if the user gives his consent.
- The link to download the official national contact tracing application should be clearly informed by the controller and the public authorities in order to avoid users using third party apps.

4. CONTACT TRACING APPLICATION ARCHITECTURES

There are two main approaches that can be used for contact tracing applications. The classification criteria consider how the server is used and what data is required by it.
There is the centralized approach, that uses a trusted server to generate ephemeral identifiers for each user. The server receives a list of all the identifiers the user encountered, only if a user is a confirmed case, and alerts those who have encountered him.

Also, there is the decentralized or localized approach that moves the core functionalities to the user's device and uses a server to hold the ephemeral identifiers of positively infected users. The device is used to generate the ephemeral identifiers, to store all the identifiers that it has received from other devices and alert the user if they have come into contact with an infected individual.

4.1 Centralized Protocols

One of the approaches of processing data for contact tracing applications is to enlist a centralized protocol, such as ROBERT and BlueTrace. Centralized protocols utilize servers where encrypted data is gathered from the aforementioned applications, through anonymous channels, and then processed. Since the health authorities have access to a number of legitimate data related to COVID – 19, they are considered a natural candidate to host such a server infrastructure. Of course, other candidates can be considered as long as they fit the criteria and they can be trusted by the public to handle such a delicate process.

4.1.1 Base Functionality

The functionality of a centralized protocol is based on the secure communication between two entities, the contact tracing applications which the users have voluntarily installed on their device(s), and the server. When these entities communicate, there should be a secure channel established as well as a way of authenticating the users. Once the connection has been established and the user has been authenticated, the applications transmit and receive anonymized ephemeral identifiers and encrypted data, to and from the server. The data from the applications have gone through some processing before being transmitted. It is important to keep the user's identity well-hidden to avoid their stigmatization in case of a positive result. In order to achieve that, only the absolutely necessary data from the user's device is being collected and then encrypted before being transmitted to the server. The server generates a list of ephemeral identifiers for each user that connects to him, then forwards them, so the user can broadcast each one for a predetermined period through the application. The application continuously scans for nearby devices that advertise themselves and stores, in a list locally, the identifiers of the people that the user has encountered. Older identifiers are removed after a period of time has passed. The server receives this data from confirmed cases. The data may also contain encrypted information such as the proximity between them, their location and the time of contact, depending on the designed implementation for calculating the personal risk score [8], [9]. The lists received from confirmed cases are being used by the server. Since the server is the one producing the ephemeral identifiers of each user, it can match them with the ones in the received lists, calculate the risk and transmit a status to the contacts at risk. The users who are notified, will decide whether they wish to visit their doctor, be tested or self-isolate.

4.1.2 ROBERT and BlueTrace Protocols

The ROBERT protocol follows the base functionality with a slight difference on how the user is notified. The server does receive the list of contact pseudonyms from the confirmed cases and calculates the personal risk for them, however, the server does not notify the contacts at risk immediately. For a user to find out whether he is at risk or not, their application is sending frequent queries to the server asking for their status. If the pseudonym from the query, is matched to the ones at risk on server, then the user is informed through the app. If they are at risk, their application is disabled until they are confirmed as COVID-free [10].

BlueTrace protocol differentiates in two areas, on what information the server stores per user and how it uses that to produce the pseudonyms, and how the contacts at risk are alerted. The user registers to the server with his phone number and the pseudonyms that the server produces for them are associated with that. This information is required in order to alert the users that had prolonged exposure to an infected person. The contact tracing process involves an interview with the confirmed case, where they are asked to recall where they have been, who they have been in contact with recently, as well as, to upload the proximity history stored in their app [11]. This information is used to adjust the proximity and duration filtering thresholds based on the confirmed case-reported location and context. The health authority then contacts individuals assessed to have a high likelihood of exposure to the disease, to provide medical guidance and care [12].

Alternative implementations of BlueTrace that do not require a phone number are possible. These might rely on push notification tokens to alert individual users [12].

4.1.3 Benefits and risks of using a centralized protocol

Utilizing a Centralized protocol has benefits, but it also hides some risks. As mentioned before, health authorities are a natural candidate to run a centralized server as they collect data from infected people and ensure that it is legitimate. Reports of false infections can cause unnecessary fear and chaos within the communities. To ensure the anonymization of the users, the server generates multiple ephemeral identifiers (pseudonyms) for each one. These pseudonyms are the output of an encryption algorithm, and they are updated in regular time frames, the frequency of which depends on how quickly the virus spreads. This frequent alternation of the user's pseudonyms ensures that he cannot be tracked and be identified by any malicious third party. However, there is a risk in the way the ephemeral pseudonyms are being created. If they are created by encrypting a static identifier and the encryption key is leaked, then the ephemeral identifiers can be deanonymized and the identity of the user become exposed. A proposal to reduce the possibility of such cases is to use rotating keys for the encryption process [13]. While user's devices use these pseudonyms to advertise themselves, they also log the pseudonyms received from anyone the user has come in contact with. But the logs recorded can differ from device to device. Defining "contacts" for the application is dependent on the technology the device uses to send and receive data. For example, by using BLE (Bluetooth Low Energy), due to different Bluetooth ranges per device, the distance recorded by them may differ or not being recorded at all. Consequently, one cannot conduct who may have infected them or may be the cause of the risk notification, just by looking at their contact logs. The risk of processing all this data in one server is data leaks. As the server collects data from confirmed cases, it may detect patterns regarding pseudonyms that appear in the logs of multiple users or that appear at the same time and/or place. In other words, it can reveal relations between different users and build social graphs for parts of the userbase. However, the leakage is for the server only, so if the server is trusted and secure, there is no disclosure at all. If the host of the server is malicious, they could install sensors to public areas, gather pseudonyms from the various users and follow their movements, depending on how densely the sensors are placed. Replay attacks can, also, be considered a risk of using centralized protocols in order to create chaos with false positives. Though this is easily solved by adding short expiration dates on the messages exchanged between users. Even if someone copies a user's broadcast message and replays it, at some point this message will not be valid anymore and the applications will ignore it [10].

4.1.4 Example of how centralized protocols function

Figure 2 shows an example of centralized topology. We have an application (app_u) that the users, Mike and Karen, install on their device(s) and a centralized server (S_c) where data is transmitted to and from. We presume that Bluetooth Low Energy technology is used for the exchange of data between user devices.

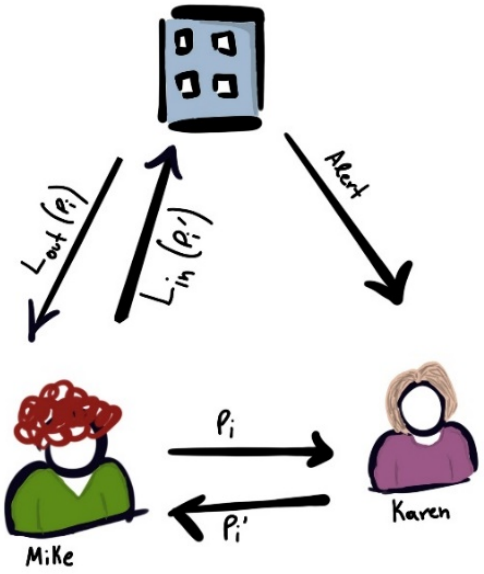

Figure 2. Centralized protocol topology

After the app_u installation, Mike's device connects to the server and receives a list of pseudonyms, $L_{out}(p_i)$. Every p_i is used by Mike's device to advertise itself for a specific period and once all the p_i from the list are used, then the device connects again to the S_c and receives new ones. When Mike's app_u encounters Karen, collects her p_i' and stores them locally in a list $L_{in}(p_i')$. If Mike is a confirmed case, he can decide whether he wishes to allow the app_u to transmit the stored $L_{in}(p_i')$ to the S_c. For the sake of this example, we assume that Mike trusts the server and forwards the $L_{in}(p_i')$. After that the S_c calculates a personal risk score for all the included p_i' based on the duration of contact, proximity and other factors. If the score exceeds a threshold, the S_c matches the p_i' with the p_i it has assigned to each user, and then alerts the users at risk by sending a push notification (alert) on their device(s). Consequently, if Karen receives such an alert, she will decide her next steps. She can self-isolate, visit a doctor or disregard the notification altogether.

4.2 Decentralized Protocols

Another approach of processing data for contact tracing applications is to use a decentralized protocol. The decentralized architecture moves the core functionalities to the user devices. This requires minimum involvement with a server during the contact tracing process. The decentralized approach is used to enhance the user's privacy by generating ephemeral and anonymous identifiers at the user's devices, thus keeping their identities hidden from other users and from the server.

4.2.1 Base Functionality

In the decentralized approach the interaction with the server is kept to a minimum. The user's device is used to generate privacy – preserving pseudonyms with a short lifetime. There pseudonyms are being broadcasted to other devices that come in close contact and are being stored locally in a list. The information stored includes the identifier, the timestamp of the contact and the received signal strength indication, that is later used to determine the proximity of the contact. The application installed on the user's device communicates with a server only to download and store in a different list the pseudonyms of all the infected users, that have agreed and uploaded their status, and to upload the used identifiers if the user is diagnosed positive. This exchange is being handled from the APIs that Apple and Google have created. The tracing process in a decentralized architecture is performed locally by the application on their device. The application compares all the identifiers, that has gathered from the contacts against the list received from the server. If there is a match between the pseudonyms, then the application calculates the personal risk score based on all the information it has gathered. Then it alerts the user via a push notification if they are at risk.

4.2.2 Google and Apple Framework, DP-3T, TCN protocols

The majority of protocols developed to help governments and health agencies reduce the spread of COVID-19, is based on decentralized functionality. Technologists, legal experts, engineers and epidemiologists have joined hands, internationally, to develop open-source protocols such as DP-3T and TCN, which are recruited by a number of applications worldwide. Given the situation, even multinational technology companies, Google and Apple, are collaborating in order to provide solutions to the pandemic. They have launched Google and Apple Framework, which enables interoperability between Android and iOS devices using contact tracing applications and uses Bluetooth technology to log the contact tracing [14].

4.2.3 Benefits and risks of using a decentralized protocol

There are some clear benefits of using a decentralized protocol. First and most importantly there is the benefit of privacy. Since all the encrypting and processing happens on the user's device his identity remains hidden. On centralized protocols we talked about having a "corrupt" server that can be used to track a user's whereabouts. In the case of decentralized protocols, there is no such trapdoor. However, the ephemeral identifiers are generated from a specific encryption key. If a malicious third party has in their possession the encryption key can decrypt the identifiers from the server response and link them together. This is mitigated from the fact that the encryption key typically changes once per day [13]. There is also the fact that the identifiers of positive diagnosed users are public. This is dangerous in case someone remembers a specific user's identifier. Once they have the list, they can recognize that the user has been diagnosed positive.

The main takeaway is that using a decentralized protocol is more secure and has more benefits than risks.

4.2.4 Example of how decentralized protocols function

Figure 3 shows an example of decentralized functionality. We have an application (app_u) that the users install on their devices. An assumed trusted server (S_{dec}) where the infected identifiers ($L_{in}P_i$') are saved and transmitted to the users' devices. We also presume that Bluetooth Low Energy technology is used for the exchange of data between user devices.

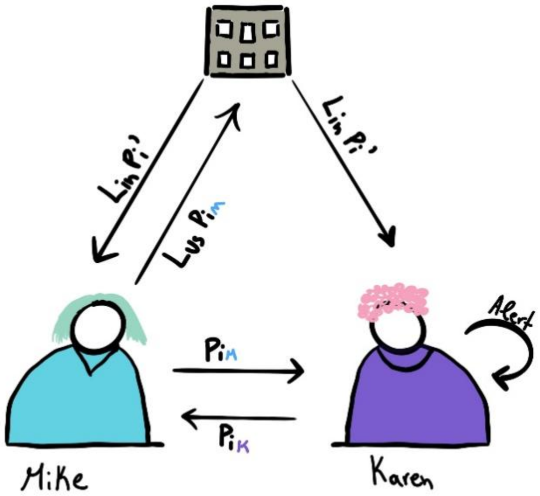

Figure 3. Decentralized protocol topology

After the app_u installation, Mike's device generates a list of ephemeral identifiers (P_{iM}) to broadcast. When Mike's device encounters Karen's, his device sends his P_{iM} to Karen's device and receives her identifier (P_{iK}). There identifiers are stored locally in a list. If Mike is diagnosed as positive, he can choose whether to upload his result to the S_{dec} along with his list of used identifiers ($L_{us}P_{iM}$). Karen's device checks periodically for an updated $L_{in}P_i$' and when it receives one, it processes the list and matches Mike's P_{iM}. The device then calculates a personal risk score according to the data it has gathered from the encounter. That includes the timestamp of the contact and the received signal strength indication. Consequently, the app_u alerts Karen in the form of a push notification that she is at risk. Again, the way Karen will act upon this alert, is up to her. She can choose to self-isolate, visit a doctor or disregard the alert.

5. DEVICE COMMUNICATION TECHNOLOGIES

A key factor for contact tracing applications is how the tracing is taking place. There is a number of technologies that can be used for this purpose. A few examples are Bluetooth Low Energy (BLE), GPS, Wi-Fi, Magnetometer, even QR codes. In this survey, we are going to focus on the two mostly used technologies in contact tracing applications: GPS and Bluetooth Low Energy.

5.1 GPS

The applications that use GPS technology for tracing, log the user's location. When the user is a confirmed case, they upload their location history, which is then distributed to the rest of the users. The location history of a user and the location histories of infected users combined, are the key factors with which the application will determine whether the user is at risk. On one hand, tracing through GPS doesn't require any communication, e.g. broadcast messages, handshakes, etc, between devices with the contact tracing application on them, which reduces the application's energy consumption. On the other, GPS as a service, is on its own a costly procedure. It drains the device's battery faster than other technologies, such as Bluetooth, and the continuous use of it can lead to device energy shortage. Since contact tracing applications are made for mobile devices and should be running as long as the device is turned on, energy shortage is an issue that is not tolerable by the users and needs to be thoroughly considered before implementation.

Another disadvantage of GPS is the high false positive rate. As a reference, widely accepted epidemiological parameter for close contact with a confirmed case, is 30 minutes at a distance of less than 2 meters [12]. GPS has an accuracy of 10 meters, which decreases in urban -especially if there are tall buildings- and underground environments, but it cannot calculate the proximity of two or more users. Think of a 3-store building, with one user per floor. All three of them have the same GPS location logged on their devices, since GPS cannot detect difference between floors of the same building (limited vertical accuracy). If one of them is a confirmed case, then the other two will be falsely notified as "at risk". Another example is to have two people on the same floor but in two separate rooms. Again, if one of them is a confirmed case then the second one will be notified as being "at risk" since GPS cannot detect the proximity and is unaware of the wall between them. A malicious user could take advantage of this weakness and, either by being a confirmed case themselves or by using the device of a confirmed case, falsely notify a number of individuals as "at risk", just by being in the same building with them.

5.2 Bluetooth

Bluetooth Low Energy technology is widely adopted like GPS. In contrast with the latter, Bluetooth is much more efficient as far as energy consumption is concerned, so it is more likely to be used for many hours on a mobile device without noticeably affecting the user's daily activities. Contact tracing applications implementing BLE for tracing, exchange messages with the user's contacts and log these encounters. When a user is a confirmed case, their encounter history is uploaded and used to determine other users' risk. Bluetooth false positive rate is lower than the one for GPS. Bluetooth can determine the proximity of two or more users by the strength of the signal when receiving a broadcast/message. If two users are close, then they both will log this encounter, however, if there is a wall between them -e.g. they are in different rooms- none of them will log any encounter since Bluetooth signal is not strong enough to surpass obstacles such as a wall. There still are some false positives due to the fact that different devices have different Bluetooth transmit radius. As a result, a user with a sensitive/powerful antenna could have logged an encounter that does not exist on the contact's device, and vice versa.

Although Bluetooth advantages over GPS, there are privacy issues that result from the proximity tracing systems. A malicious user [15]:

a) with a powerful antenna can trigger false alerts about encounters with an infected person that do not reflect real-world physical proximity. For false alerts to occur, the malicious user should ensure that the interactions between the devices, are flagged as at-risk events. To do so, they either are a confirmed case themselves, they are using the device of a confirmed case, or have hijacked/bribed the health authority to trigger the contact tracing.

b) can disrupt the contact discovery between users through noise injection in the radio channel. If the malicious user has modified their contact tracing application to broadcast different pseudonyms every minute or less, they can "overcrowd" the channel and the devices in the area will store all the different pseudonyms, while discarding the older ones, due to memory capacity. As a result, the contact history of the neighboring devices will be full with pseudonyms belonging to the malicious user and the contact discovery is much more difficult.

c) that actively goes war driving, can identify locations with infected people present. A malicious user could conclude as to who is the individual who infected them or narrow down the possible confirmed case(s) to a group of individuals or locations. If the malicious user has many devices and accounts, they can visit different locations with different devices. If they are alerted, they can check which devices are also alerted and conclude as to where they may have been infected and by who, considering the number of individuals at that specific area.

6. PRIVACY AND SECURITY ISSUES

Despite the choice of architecture and communication technology, any contact tracing application should follow the specifications provided by EDPB and GDPR to the point. These guidelines were designed specifically to ensure that the privacy of the user will not be violated in any way. If at least one guideline is not taken into consideration during the application's implementation, then the user's privacy is at risk.

6.1 Privacy Concerns

It is not easy for the public to accept an application that requests access to their personal data, blindly. There are always concerns regarding their privacy and the safety of their personal information. Some of these concerns are the below:

- **Location Monitoring:** Location data are important to a user. They indicate their "common" places, such as home and work, as well as their habits. By collecting the location history of a user, one can pinpoint the places they visit, the transport they use, the people they meet frequently (roommate, partner, relatives) or scarcely, more or less their routines. These routines can be used to create a social graph for an individual, which is not only undesirable but also may lead to the identification of the individual. For example, India has followed this approach for contact tracing despite the concerns of the public.
- **Data Collection:** Apart from the location, some applications collect unnecessary data from the users. For example, BeAware app in Bahrain collects the location, national id number, contact, demographic, health and travel information. These are information that no user would like to share or transmit through the network as it can identify them. There is also the issue of collecting location data when the application uses other wireless technologies such as Bluetooth, to do the tracing.
- **Transparency:** Once all the data is collected, there is the concern of where they are stored and how they are processed. When deploying a contact tracing application, there must be transparency for the process of data, the data flows, the databases used, the policies implemented and the code. Knowing how the application works makes it more reliable and more privacy-proof.
- **Data Destruction:** It is important that the collected data must be deleted once it is no longer needed and not used for other purposes. This means two things, 1) user data should be automatically deleted after a predefined period, and 2) once the contact tracing application is discontinued, all the stored data must be deleted from the appointed entity.
- **Free Will:** Some countries such as China, Qatar, Russia and Philippines enforce the adoption of their contact tracing applications to their countries. Under no circumstances should a contact tracing application be mandatory. Considering the location monitoring, the amount of unnecessary data collected, the various concerns for the processes of the application, the user must be free to choose whether they will adopt the application or not and whether they will give their consent for the application to access to their personal information on the device.

6.2 Security Attacks

Apart from the privacy concerns, contact tracing applications are vulnerable to security attacks. Some were mentioned in the protocols (Centralized - Decentralized), Bluetooth and GPS technologies in the previous sections. In this section some of the possible security attacks that one can launch against contact tracing applications, are presented [16]–[20].

6.2.1 Replay Attacks

The application sends and receives messages. Depending on the protocols implemented and the technologies used, the data contained in the aforementioned messages vary. A Replay attack is very simple to launch. It is a version of “Man in the middle attack”. A malicious user can capture the messages broadcasted to and from one or more users and then re-send them at the same or another location. The purpose of this attack is to make users store misleading contact data on their devices and result in false “at risk” alerts. If the malicious user has also placed antennas, they can extend the area they influence with their transmissions.

As mentioned in section 3.1.3, this is easily solved by adding short expiration dates on the messages exchanged between users. Even if someone copies a user’s broadcast message and replays it, at some point this message will not be valid anymore and the applications will ignore it [10].

6.2.2 Denial of Service - Resource Drain Attack

Denial of Service attacks aim to overload the system by utilizing all its available resources, and rendering it inoperable. In the case of contact tracing applications, the attack is based on injecting fake encounters in the contact tracing process. Replay attacks, for example, can be one way of spreading false encounters in a large area(s). The more messages are sent, the more storage and battery is consumed from the user’s device. If the message is valid then battery and storage are consumed, otherwise only battery is consumed. This results to low performance of users devices. Once one of the users is tested positive, if they upload their data, all the misinformation will be uploaded to the server. This can result in increasing the processing timestamp at the server, to the point of having long delays or even render the server unavailable. This kind of attack can affect both centralized and decentralized approaches.

A possible solution to such attacks is filtering the received messages by the device’s system before waking up the contact tracing application. For example, if a message is invalid, then the following messages with the same information and pseudonym should be ignored. If a message is valid then it is handled by the application but duplicates received should be ignored by the system. If the rate of incoming messages, the battery consumption or the storage consumption suddenly increases drastically, then the system can inform the user and consult him to move away from the area or report potential attack.

6.2.3 Bluesnarfing

In contrast to Replay and Denial of Service attacks where the malicious user would only capture and re-transmit already sent messages with no regard as to what they contain, Bluesnarfing is a security attack that can gain access to the user's sensitive data by forcefully establishing a connection with a Bluetooth-enabled device. Any data stored in the device's memory, such as photos, videos, files, appointments, even the International Mobile Equipment Identity (IMEI), can be accessed and stolen without the owner's knowledge.

To avoid such attacks, it is simple. If the device is invisible to other devices and/or it allows connections only from known devices, then it cannot be affected by Bluesnarfing attacks.

6.2.4 Enumeration

This attack can affect contact tracing applications that utilize Centralized protocols. In a centralized approach, as discussed earlier in the paper, the user's device communicates with the server to connect to it, to receive new pseudonyms and to transmit the list of pseudonyms logged during contacts if the user is tested positive. A message sent for establishing connection with the server and a message sent to the server including the logged contacts, differ on the size. It is expected that the latter will be bigger that the former. As a result, a malicious user can observe this difference in size and estimate the number of infected users in an area. This number cannot be absolute as the upload of contact history from a confirmed case is volunteering.

A simple solution is to add junk information at the end of the request for connection with the server, in order to have similar size with the message uploading the user's logs.

6.2.5 Carryover Attack

Contact tracing applications that use Bluetooth technologies, have Bluetooth MAC addresses and temporary identifiers. Both of the above are randomized after a short time in order to avoid device tracking. Carryover attack is launched when a malicious user wants to keep track of a device even after the anonymous ID expiration time. This attack is possible when the frequencies of changing Bluetooth MAC address and temporary identifier are not synchronized. For example, we will assume that the application changes temporary identifiers every 12 minutes and Bluetooth MAC addresses every 5 minutes. A malicious user can link the different MAC addresses of a device during the lifetime of each temporary identifier. Similarly, the former can link the different temporary identifiers during the lifetime of a Bluetooth MAC address.

The solution to such an attack is to completely synchronize the changes in temporary identifiers and MAC addresses.

6.2.6 Trolling Attacks

Trolling attack is when a malicious user that is or expects to be tested positive, attaches their device to a carrier that moves around and advertises itself to other devices. Consequently, non-affected users will be notified as having been closed to an affected person, conduct tests to ensure whether they are affected or not, and waste resources of health authorities. This can lead to the loss of public trust for contact tracing applications reliability and the diagnosis procedure.

A user that has received an alert will take a test at a health authority to find out if they are affected or not. A solution would be for the health authorities to gather the logged proximity identifiers of the potential cases devices and check for abnormal appearances of the same pseudonym/diagnosis key in different locations at the same or short periods of time. This way they can locate the malicious user key and publish it so that the device's ignore messages received from the malicious user.

6.2.7 Tracking and Deanonymization Attacks

In section 4.2, we mentioned that a malicious user can go on war driving to identify locations with infected users. Depending on the number of people in the area at the time the malicious user was there, they can even identify the infected person. This attack violates user's privacy. Let's assume we have two scenarios, one, the user has multiple accounts and visits different places with different devices, and two, they use only one device and when they meet a person (and the contact is logged) then they turn off the device so no more encounters are logged. The second scenario is exactly like in 4.2, but in the first scenario the malicious user can immediately identify an infected person if the contact logged is tested positive in the future.

One suggestion is to have k-anonymity. More specifically, the idea of k-anonymity is to always have k devices in an area, whether those are real or fake. If a device is alone in broadcast proximity, then when advertising itself, it sends k-1 random temporary identifiers (as fake devices in the area) along with its temporary identifier. By doing this, the malicious user visiting the individual has logged k temporary identifiers instead of one, and so, if the individual is tested positive, the malicious user cannot identify them.

6.2.8 Screen Lock Attack or Ransomware

This attack is a result of downloading fake contact tracing applications that aim to lock user's device and steal data such as photos, videos, files, bank details and other private user information. An example of Ransomware is the CovidLock application that locks the user out of the device by changing their password and demanding a ransom to unlock, otherwise it will delete or publish all user's data to social media.

It is due to attacks like these that the official sites for downloading contact tracing applications should be published by the governments under the context of transparency. If the public knows the official sites, then installation of applications and ransomware from third party stores and shabby websites can be avoided. Also, the use of anti-virus can help prevent such attacks.

6.2.9 Bluebugging

Older Bluetooth devices, usually those using Bluetooth Classic, have a security flaw that allows a malicious user to gain access to the device. This attack is called Bluebugging. The goal is to get unauthorized access to the targeted device and be able to run commands, make phone calls, etc.

If the Bluetooth is disabled when not in use then the attack can be avoided. Also, if the device scans incoming messages for possible infections Bluebugging can be prevented.

6.2.10 Jamming Attacks

Jamming Attacks are a kind of Denial-of-Service attacks. Their purpose is to prevent a device from being able to send signals on a channel by occupying it. These attacks are affecting location-based contact tracing applications by overpowering the GPS signal, so that it can’t be tracked and received by the GPS receiver.

To avoid jamming attacks the device could transmit signals to different channels and frequently change between them, so even if some channels are jammed the rest can still be used. Another technique would be to use notch filters or adaptive notch filters for GPS attack detection.

6.2.11 Spoofing Attacks

A Spoofing Attack is a practice employed by a malicious user to deceive a system to perceive something as something that it is not. In the case of contact tracing applications, spoofing attack is when a malicious user uses radio signals near a device to interfere with the GPS signals so that no data or inaccurate coordinates are transmitted. Consequently, this attack also affects location-based contact tracing.

To counter GPS spoofing the device needs to monitor and record the average GPS signal strength. For the malicious user to interfere with the GPS signals, they should transmit a higher power signal to cover the former one. As a result, if the observed signal strength exceeds some threshold, the device should alert the user.

7. APPLICATIONS AROUND THE WORLD

During the last 2 years of the pandemic, more than 50 contact tracing applications have been developed worldwide. Some have based their functionality on centralized systems and others on decentralized ones. Examples of such applications are TraceTogether developed for Singapore, WeTrace developed for Philippines, MyTrace developed for Malaysia, StopCovid or TousAntiCovid developed for France, etc. [21]–[26]

An ideal contact tracing application must have certain key points in order to be widely adopted from the general public:

- Optional installation and use,
- The code should be open source and allow reviews and contribution, to avoid security issues and secure the applications against malicious attacks,
- Require as little information as possible from the users. No unnecessary information such as phone number, address, id card number, nationality, gender, etc should be collected from the users, to protect their privacy,
- Transparency between governments and the public, as to how the applications are functioning, what data are being collected, how they are being processed and how long the user's data are kept,
- Have a low false positive rate. The lower the ratio, the more trustworthy the application's alert,
- Interoperability, being able to travel from one country to another without losing the functionality of your contact tracing application.

Many of the developed applications failed at one or more of the above key points. As a result, they were not trusted by the majority of the general public. In the case of the tracing apps, low trust means low uptake, and, consequently, low efficiency [21].

Each one of the BeAware(Bahrain), Alipay Health Code(China), COVI-ID(South Africa), CovTracer(Cyprus), Corona Tracer BD(Bangladesh), Ehteraz(Qatar), NHS App(UK), Stopcoronavirus. My Contacts(Russia) collect some or all of the below: National ID Number, Contact Information, Demographic Information, Health Information, Travel Information, Phone number, unique user ID, Biometric Information, Post Code District, Venue Check-in Data. Such sensitive information does not encourage the trust of the users and, based on section 2, are not vital for the contact tracing and the calculation of the personal risk. What's more, China, Russia and Qatar have made their applications mandatory for the public, while they have no privacy framework, e.g. Apple/Google Framework, to back them up.

In some countries, such as in Czechia, Poland, Hungary, Slovenia and Spain, data protection impact assessments were not conducted or only in a limited manner and had to be repeated after the launch of the app, or data controllers did not consult the data protection authorities before launching the app. This is not in line with obligations set by the GDPR [21]. A number of EU applications are now discontinued while others are still under development, Table 1.

Another reason why some of the contact tracing applications have failed, is the lack of transparency and public trust. In countries, such as Ireland, Finland, Denmark, and Germany, there is an over 30% adoption rate of these apps. The reason is that all relevant information, as well as the code of the applications, were publicly available and the government has conducted public debates, to ensure that the people know why and how the tracing works. In other words, they gained the public trust. In most of the EU countries though, the adoption rate is below 20%! This is understandable when you have a new technological solution provided, that many may not be familiar with, without providing adequate information or public debates and without proof of efficacy [21].

Furthermore, there is also the case of false positive rate. An accurate risk assessment depends on accurate data. Location data (GPS) is not accurate under certain circumstances, especially in highly populated areas with tall buildings and underground areas. Unfortunately, location data can be used from whoever has access to it for more purposes than tracing. A malicious person or party with access can create social graphs and/or stigmatize individuals by finding out their address, work, etc. However, technologies that trace contacts based only on the distance from the user (Bluetooth) are more secure and private and should be preferred when designing a contact tracing application.

During the lockdowns that have been enforced the last 2 years, travelling from country to country has not been an easy task. Since there was a number of contact tracing applications deployed around the world, there was a need for interoperability. In autumn of 2020, the EU interoperability gateway was launched in order to securely exchange information between national apps based on decentralized architecture. Up till 2021, 17 apps were already added to the gateway and were able to function across borders. Today, 13 apps out of the 17 are active [27], Table 2. Unfortunately, France and Hungary cannot be added to the gateway since their approaches are based on centralized architecture.

In 2021, a research was conducted, gathering all the known contact tracing applications worldwide up to that period, Table 4 [22]. The purpose of the research was to determine whether the developed applications have strong privacy protection for the user's data. Each one was evaluated with a score from 0 to 10, on the basis of 5 axes: how the tracing is taking place, what personal data are collected, where they are stored, who has access to them and if there is a privacy framework implemented. 14 apps have scored 0! All of them use GPS location services, unnecessary amounts of sensitive personally identifiable data, allow third-party or otherwise questionable access to that data, store the data on centralized servers, and do not employ any privacy-preserving framework for contact tracing [22]. There were a few that scored an 8, Germany with Ito that scored 9 and Switzerland with SwissCovid-App that scored a 10. SwissCovid-App fairly respects the user's privacy. It is based on decentralized architecture with the user being the only one having access to the data collected. It uses Bluetooth technology to trace contacts, collects zero personal data and employs the privacy-preserving contact tracing frameworks DP-3T and Apple/Google Framework.

What we can take away from this is, if an application checks all the privacy-preserving rules it will be adopted and trusted from the public. As a result, the use of technology for contact tracing will be an immense help at handling the COVID-19 crisis.

Table 1. EU discontinued and under development applications

Country	Status
Austria	Discontinued
Cyprus	Discontinued
Czechia	Discontinued
Denmark	Discontinued
Greece	Under development
Poland	Discontinued
Romania	Under consideration
Slovakia	Under development

Table 2. Active EU national applications added to EU interoperability gateway

Country	Name
Belgium	Coronalert
Croatia	Stop COVID-19
Finland	Koronavilkku
Germany	Corona-Warn-App
Ireland	COVID Tracker
Italy	Immuni
Latvia	Apturi Covid
Lithuania	Korona Stop LT
Malta	COVIDAlert
Netherlands	CoronaMelder
Norway	Smittestopp
Slovenia	#OstaniZdrav
Spain	Radar Covid

7.1 Who else may access the data?

As shown in Table 4, each app has one or more parties that have access to the collected data. They are governments, health officials or other third parties, such as universities, research organizations, marketers/advertisers, etc. In some cases, e.g. universities, the access to the collected data can be beneficial as it can be used for research purposes. In other cases, though, allowing advertisers, marketers, private companies, auditors or any other third party not immediate concerned with the contact tracing applications or their functionality, constitutes a danger to the users' privacy. Let us consider **two cases** where we assume that **third parties have access to the data**: the application collects **zero** data from the user, the application collects **at least one** personal information about the individual, whether that is their location, identification number, address, demographic / contact / travelling / health information, etc.

The first case is a happy scenario for the users' privacy. If the application does not collect any data, then there is nothing to be exploited and, consequently, nothing for beneficial research to reduce the spread of COVID-19. It has its pros and cons, but it is the ideal standard for contact tracing applications.

In the second case, the application must be designed very carefully in order to avoid data leaks that compromise the user's privacy. When collecting personal information, they must go through an anonymization process. If there is no anonymization or the algorithm used is not strong enough and deanonymization is possible, then data exploitation can take place. If used for malicious purposes, any entity with access can stigmatize and/or isolate individuals or minorities or even publish these data to other entities. Also, as aforementioned, there is the issue of transparency. The public must be informed as to who has access to the collected data. Therefore, having third parties such as marketers and advertisers, does not encourage the public to adopt and voluntarily grant access to the application. In other words, apart from governments and health officials, third parties must be entities that inspire trust to the people.

7.2 Permissions

Applications, as a rule, must ask from the user to give the minimum number of permissions required for it to function. If an application requests more permissions than necessary, then the user will be reluctant to give access as well as they will start questioning the app and possibly not use it. The same logic applies to contact tracing applications. Depending on the design of the contact tracing application, it may require access to the camera (QR codes), Bluetooth, user's location (GPS) or a combination of those to function accurately, since this is the minimum required for calculating user's risk. Extra permissions, other than the above, may raise public suspicion. By requesting access to microphone, storage, phone calls, it is insinuating that personal information from the user's device can be collected and accessed by any entity-ies managing the collected data. This is a threat to the user's privacy as such sensitive information may lead to exposing the identity of an individual. The risk is higher when the aforementioned entities include third parties like mentioned in section 5.1.

7.3 Adopted Methodology

Based on Table 4, we looked through the permissions requested, as well as, the libraries used from each application, from the lowest to the highest score, to discover if they are privacy proof. The tool we used was the https://exodus-privacy.eu.org/en/ website. This tool has stored most of the applications that have been published in Google Play Store, even if they are not available anymore. Searching by name, it finds the application, provides a link to store and then catalogs its trackers and permissions required. It also points out the dangerous permissions, as well as what kind of access each permission allows. Unfortunately, not all applications from Table 4 were available, however, we found the majority of them.

7.4 Findings

In Table 3, we present our findings. At first glance, we observe that few applications have no trackers at all, while most of them have at least one for analytics, crashes and/or push notifications. Common trackers are Google, Microsoft and Huawei, but there are also 4 less common ones (AltBeacon, OneSignal, Bugsnag, OpenTelemetry). AltBeacon is a protocol specification is used by devices to advertise their proximity to nearby devices [28]. OneSignal is mechanism for push notifications. In other words, it's a tool through which a server or the device itself can inform the user of their personal risk [29]. Bugsnag is a tool for monitoring applications' stability and helping developers make data-driven decisions on whether to implement new features or fix bugs [30]. OpenTelemetry is a collection of tools, APIs, and SDKs in order to instrument, generate, collect, and export metrics, logs, and traces [31]. AltBeacon and OneSignal are not dangerous trackers since they don't use or access any of the personal information of the user neither transmit it. Bugsnag and OpenTelementry do collect data of the application, however it is data related to the application's functionality in order to ensure its stability, and not user's personal information.

Regarding the permissions, the majority of the applications in Table 3, requests access to the device's Bluetooth regardless of whether they collect data based on GPS, Bluetooth or other technology. Same goes for location permission. Some examples are BeAware, CovTracer, Shlonik, NZ Covid Tracer and PeduliLindugi application. As mentioned in section 5.2, if the permission is not vital for the application's functionality, then it should not be requested. Apart from Bluetooth and location permissions, we observe a number of permissions that may alert the user. The most common are the accesses to settings and storage, both external and internal (BeAware, CovTracer, Aarogya Setu, etc). The applications requesting this, all but one (Malaysia – MyTrace), collect a lot of personal information from the user's device. This is one of the reasons they have a low score in Table 4. Other applications request access to the camera. In applications such as NZ Covid Tracer and NHS App where QR codes are used for tracing, the use of the camera is understandable. However, TraceTogether, TousAntiCovid, Shlonik, etc, should not be having access to the device's camera. Other rarer but still alerting permissions listed are phone state, calls, calendar and record audio. The only extra permissions that are acceptable while not needed for tracing, are biometric and fingerprint ones. Only 4 applications in Table 3 have this permission. Biometrics/Fingerprint are stored locally and none of these 4 applications request access to internal storage or to storage in general. In other words, they don't collect these data. As for the reason of their existence, it is for the quick login of the user to the application and since it is something common to most applications nowadays, it is not alarming to the user. As long as the permissions of those applications do not change, they do not constitute a threat to the user's privacy as is.

Table 3. Permissions and Trackers

Country	Application Name	How Does It Work	Trackers	Permissions
Bahrain	BeAware	GPS location data	AltBeacon, Google Firebase Analytics	• Location • Bluetooth • Calendar • External Storage • Settings
Bangladesh	Corona Tracer BD	Bluetooth, GPS location services	-	• Location • Bluetooth • Phone State
Cyprus	CovTracer	GPS	Google Firebase Analytics	• Location • Bluetooth • External Storage • Settings
India	Aarogya Setu	Bluetooth/GPS location tracking	Google CrashLytics, Google Firebase Analytics	• Location • Bluetooth • Camera • External Storage
Kuwait	Shlonik	GPS	Google Firebase Analytics, Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Center Crashes, OneSignal	• Location • Bluetooth • Camera

				- External Storage - Phone State - Settings
Qatar	Ehteraz	GPS/Bluetooth	AltBeacon, Google AdMob, Google Analytics, Google CrashLytics, Google Firebase Analytics, Google Tag Manager, Huawei Mobile Services (HMS) Core	- Location - Calls - External Storage - System Alert Window
Bulgaria	ViruSafe	GPS	Google CrashLytics, Google Firebase Analytics	- Location
Columbia	CoronApp	Self-reported data, location data	Google Firebase Analytics, Huawei Mobile Services (HMS) Core, OneSignal	- Settings
New Zealand	NZ Covid Tracer	QR Codes	Google Firebase Analytics, Microsoft Visual Studio App Center Crashes	- Bluetooth - Camera - Biometrics/Fingerprint - Settings
Norway	Smittestopp	Bluetooth/GPS location services	Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Center Crashes	- Bluetooth - Settings
Georgia	Stop Covid/NOVID20	Bluetooth/GPS location data	Google CrashLytics, Google Firebase Analytics	- Location - Bluetooth - Record Audio
Iceland	Rakning C-19	Location data	Bugsnag, Google Firebase Analytics, Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App	- Location - External Storage

			Center Crashes	• Storage
Poland	ProteGO Safe	Bluetooth	Google CrashLytics, Google Firebase Analytics	• Bluetooth
Indonesia	PeduliLindugi	Bluetooth	Google CrashLytics, Google Firebase Analytics, OpenTelemetry (OpenCensus, OpenTracing)	• Location • Camera • External Storage
France	TousAntiCovid	Bluetooth	-	• Location • Bluetooth • Camera
Singapore	TraceTogether	Bluetooth	Google CrashLytics, Google Firebase Analytics, Huawei Mobile Services (HMS) Core	• Location • Bluetooth • Camera • External Storage
UAE	ALHOSN	Bluetooth	-	• Camera
UK	NHS App	Bluetooth/QR Codes	Google Firebase Analytics	• Location • Camera • Biometrics/Fingerprint • Calendar • External Storage
Czech Republic	eRouška	Bluetooth	Google CrashLytics, Google Firebase Analytics	• Bluetooth
Malaysia	MyTrace	Bluetooth	Google CrashLytics, Google Firebase Analytics	• Location • Bluetooth

				• External Storage • Storage
Northern Ireland	StopCovid NI	Bluetooth	-	• Bluetooth
Finland	Koronavilkku	Bluetooth	-	• Bluetooth
Netherlands	CoronaMelder	Bluetooth	-	• Bluetooth
Australia	COVIDSafe	Bluetooth	Google Firebase Analytics	• Location • Bluetooth
Austria	Stopp Corona	Bluetooth	-	• Bluetooth
Italy	Immuni	Bluetooth	-	• Bluetooth
Latvia	Apturi Covid	Bluetooth	Google CrashLytics, Google Firebase Analytics	• Bluetooth
Brazil	Coronavirus - SUS	Bluetooth	Google Firebase Analytics	• Bluetooth
Canada	COVID Alert	Bluetooth	-	• Bluetooth • Camera
Gibraltar	Beat Covid Gibraltar	Bluetooth	-	• Bluetooth
Ireland	COVID Tracker Ireland	Bluetooth	-	• Bluetooth • Camera
Portugal	STAYAWAY	Bluetooth	-	• Bluetooth
Saudi Arabia	Tabaud	Bluetooth	Google CrashLytics, Google Firebase Analytics	• Bluetooth

Spain	Radar COVID	Bluetooth	-	• Bluetooth • Biometrics/Fingerprint
Uruguay	Coronavirus UY	Bluetooth	Google CrashLytics, Google Firebase Analytics, Huawei Mobile Services (HMS) Core, OneSignal	• Bluetooth • Camera • Record Audio • Settings
Switzerland	SwissCovid-App	Bluetooth	-	• Bluetooth • Biometrics/Fingerprint • Camera
Jersey	Jersey Covid Alert	Bluetooth	-	• Bluetooth

8. CONCLUSIONS

One simple question must be answered while designing a contact tracing application: How we can protect the user by ensuring their privacy, while achieving reliable contact tracing.

Based on all the above, if we were asked to make suggestions for the under-development contact tracing application of Greece, our proposition would be to develop an application which features resemble the ones of Switzerland's application. First and foremost, the use of the app must be optional. The users should download the app and give access to their data, voluntarily. This is in order to avoid unnecessary data collection and lose the public trust. To ensure the users' privacy the decentralized architecture is preferred as it is more secure, because no data need to leave the user's device at any moment. Since no data, other than the pseudonyms, needs to be exchanged during a contact, the most suited technology is Bluetooth Low Energy. It does not consume a lot of the device's battery and the distance of the contact is determined by the strength of the signal. As a result, there is high accuracy on contact tracing and low chance of receiving false alerts from the application. To keep up with the public trust, the application should not request access or collect any personal information from the user, apart from the exchanged pseudonyms in case of a confirmed case. Additionally, in order for the application to be secure it must employ at least one of the security frameworks, most preferably the Apple/Google framework, as it is developed by two multinational companies that keep their code public, accept reviews, privacy concerns and update their framework accordingly. Moreover, we need to take into consideration that Greece is a popular destination for tourists. Consequently, it should follow the technical specifications of interoperability and be added to the EU interoperability gateway. When deploying the application, it is important that the government makes public any related information, as well as the source code, and present to the public how the application functions so that it is understandable by everyone. By earning the public trust, more people will adopt the application. With high adoption, there will be high efficiency and the tracing will be much easier. Lastly, the official stores / sites (App Store, Play Store etc.) from where anyone can download the official application, should be known to the public in order to avoid any malicious side loading.

With those suggestions in mind, if any new sanitary threats or other public crisis arise in the future, we should handle each possible technological solution with a high level of respect to the user's privacy and always prioritize the protection of their data.

Table 4. Contact Tracing Applications Worldwide

Country	Scor e	App	Data Collected	How Does It Work	Privacy Framework	Where Is Data Stored	Who Accesses Data
Bahrain	0	BeAware	Location, National ID Number, Contact Information, Demographic Information, Health Information, Travel Information	GPS location data	No	Centralized Servers	Health Officials, Relevant Official Bodies, Third part entities
Bangladesh	0	Corona Tracer BD	Phone number, National ID number, unique user ID	Bluetooth, GPS location services	No	Centralized Servers	Health Officials, Information and Communication Technologu Division
China	0	Alipay Health Code	Contact Details, Location, Medical Information, Demographic Information, Travel Information	QR codes/User reported location info	No	Centralized Servers	Government, Law Enforcement

Cyprus	0	CovTracer	Location, Contact Details, Demographic Information, Health Information	GPS	No	User's Device	Research Centre of Excellence on Information and Communication Technologies
Ghana	0	GH COVID-19 Tracker App	Contact Details, Location, Demographic Information	Bluetooth/GPS location services/Self-reported data	No	Centralized Servers	Government
India	0	Aarogya Setu	Contact Details, Location, Demographic, Travel Information	Bluetooth/GPS location tracking	No	Centralized Servers	Government
Kuwait	0	Shlonik	Location, National ID number	GPS	No	Centralized Servers	Health Officials, Central Agency of Information, Telecom Provider
Peru	0	PeruEnTusManos	GPS Location data	GPS	No	Centralized Servers	Peruvian Government
Qatar	0	Ehteraz	Location, National ID number, Health Information, Contact Details	GPS/Bluetooth	No	Centralized Servers	Health Officials, Ministry of Interior

Russia	0	Stopcoronavirus. My Contacts	Contact Details, Location, Travel Information, Demographic Information	GPS/QR Code	No	Centralized Servers	Law Enforcement Authorities
Slovakia	0	Zostan zdravy	Contact Details, Location, Medical Information	GPS location services	No	Centralized Servers	Private Company, Government,
South Africa	0	COVI-ID	Contact Details, Medical Information, Biometric Information, Demographic Information	QR Codes	No	Centralized Servers	Private Companies, Third Party Entities (including marketers/advertisers) , Health Officials
South Korea	0	Corona 100m *	Location, Contact Details	Location services	No	Centralized Servers	Private Company
Turkey	0	CoroWarner	Undisclosed	Bluetooth/GPS location services/Telecom location data	No	Undisclosed	Undisclosed
Bulgaria	1	ViruSafe	Contact Details, Location, Demographic	GPS	No	Centralized Servers	Health Officials

			Information, Health Information				
Columbia	1	CoronApp	Contact Details, Location, Medical Information, Demographic Information, Travel Information	Self-reported data, location data	No	Centralized Servers	Health Officials
Morocco	1	Trackorona	Undisclosed	Unknown	No	Undisclose d	Relevant Official Body
New Zealand	1	NZ Covid Tracer	Contact Details, Demographic Information	QR Codes	No	Centralized Servers	NZ Ministry of Health
Norway	1	Smittestopp	Contact Details, Location	Bluetooth/GPS location services	No	Centralized Servers	Health Officials
Philippines	1	WeTrace	Contact Details	GPS locations services	No	Centralized Servers	Health Officials
Thailand	1	Mor Chana	Contact Details, Location	Bluetooth/GPS	No	Centralized Servers	Health Officials
Argentina	2	CoTrack	Location, Medical Information, Travel	GPS	No	User's Device	Health Officials

			Information				
Georgia	2	Stop Covid/NOVID20	Contact Details, Location, Device Information	Bluetooth/GPS location data	No	User's Device	Relevant Official Body
Iceland	2	Rakning C-19	Contact Details, Location	Location data	No	User's Device	Relevant Official Body
Israel	2	HaMagen	Location	GPS location tracking	No	User's Device	Health Officials
Jordan	2	Aman	Location	GPS/Bluetooth	No	User's Device	Health Officials
Poland	2	ProteGO Safe	Contact Details, Demographic, Medical Information	Bluetooth	No	Centralized Servers	Health Officials, Relevant Official Bodies, Private Companies
Indonesia	3	PeduliLindugi	Contact Details, Device Information	Bluetooth	No	Centralized Servers	Relevant Official Body
France	4	StopCovid (Rebranded as TousAntiCovid) *	User ID, Demographic Information	Bluetooth	ROBERT Protocol	Centralized Servers	Third-party hosting provider
Hungary	4	VirusRadar	Contact Details	Bluetooth	No	Centralized Servers	Public Health Officials
North Macedonia	4	StopKorona!	Contact Details	Bluetooth	No	Centralized Servers	Health Officials

Singapore	4	TraceTogether	Contact Details, "Identification Details"	Bluetooth	BlueTrace	Centralized Servers	Health Officials, Law Enforcement Authorities
Tunisia	4	E7mi	Contact Details	Bluetooth	No	Centralized Servers	Health Officials
UAE	4	ALHOSN	National ID number, Contact Details	Bluetooth	No	User's Device	Health Officials
UK	4	NHS App *	Post Code District, Venue Check-in Data	Bluetooth/QR Codes	Apple/Googl e	User’s Device	Health Officials
Czech Republic	5	eRouška	Contact Details	Bluetooth	No	User’s Device	Health Officials
Malaysia	5	MyTrace	None	Bluetooth	No	Centralized Servers	Ministry of Health
Northern Ireland	5	StopCovid NI	Age, Full postcode, Health information	Bluetooth	Apple/Googl e Framework	User's Device	Health and Social Care Northern Ireland (HSCNI), Public Health England, Universities, Auditors, Research Organizations
EU	6	COVID19 Alert	None	Bluetooth	No	User’s Device	Relevant Official Body
Finland	6	Koronavilkku	Phone number	Bluetooth	Apple/Googl e	User's Device	Social Insurance Institution
Netherland	6	CoronaMelder	None	Bluetooth	DP-3T	User's	Unknown at this time

s						Device	
Vietnam	6	Blue Zone	None	Bluetooth	No	User's Device	Health Officials
Australia	7	COVIDSafe *	Contact Details, Demographic Information	Bluetooth	BlueTrace	User's Device	Health Officials
Austria	7	Stopp Corona	Contact Details	Bluetooth	DP-3T	User's Device	Relevant Official Bodies
Italy	7	Immuni *	Demographic Information, IP address	Bluetooth	Apple/Google	User's Device	Health Officials
Latvia	7	Apturi Covid	Contact Details	Bluetooth	Apple/Google Framework	User's Device	Health Officials
Belgium	8	B-fence	None	Bluetooth	DP-3T	User's Device	Relevant Official Bodies
Brazil	8	Coronavirus - SUS*	None	Bluetooth	Apple Google	User's Device	Ministry of Health
Canada	8	COVID Alert *	None	Bluetooth	Apple/Google Framework	User's Device	Health Officials
Estonia	8	Hoia	None	Bluetooth	DP-3T/Apple & Google	User's Device	Health Officials
Gibraltar	8	Beat Covid Gibraltar	None	Bluetooth	Apple/Google Framework	User's Device	Health Officials
Ireland	8	COVID Tracker App	None	Bluetooth	Apple/Google	User's Device	Health Officials
Japan	8	Contact-Confirmation	None	Bluetooth	Apple/Googl	User's	Health Officials

		Application (COCOA) *			e	Device	
Portugal	8	StayAway Covid *	None	Bluetooth	DP-3T	User's Device	Health Officials
Saudi Arabia	8	Tabaud	None	Bluetooth	Apple/Google	User's Device	Ministry of Health
Spain	8	Radar COVID *	None	Bluetooth	DP-3T	User's Device	Health Officials
Uruguay	8	CoronavirusUY	None	Bluetooth	Apple/Google	User's Device	Ministry of Public Health
USA	8	Novid	None	Bluetooth	TCN	User’s Device	Health Officials
Germany	9	Ito	None	Bluetooth	TCN	User’s Device	Health Officials
Switzerland	10	SwissCovid-App	None	Bluetooth	DP-3T/Apple & Google Project	User's Device	User Only
Jersey		Jersey Covid Alert	unknown	Bluetooth	Apple/Google Framework		unknown

* Official National App

ABBREVIATIONS - ACRONOMIES

EDPB	European Data Protection Board
GDPR	General Data Protection Regulation
BLE	Bluetooth Low Energy
API	Application Programming Interface
GPS	Global Positioning System
Wi-Fi	Wireless Fidelity
QR	Quick Response
MAC	Medium Access Control

REFERENCES

[1] "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," Apr. 2016.

[2] J. Bahrke, C. Wigand, K. Kolanko, and G. Mercier, "Guidance to ensure full data protection," Apr. 16, 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_669 (accessed Oct. 16, 2021).

[3] European Data Protection Board, "Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak," Apr. 2020.

[4] "DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic commu-nications sector (Directive on privacy and electronic communications)," Brussels, Jul. 2002.

[5] "What is Anonymization? - Definition from Techopedia." https://www.techopedia.com/definition/28007/anonymization-data (accessed Oct. 11, 2021).

[6] K. Finch, "A Visual Guide to Practical Data De-Identification," Apr. 27, 2022. https://fpf.org/blog/a-visual-guide-to-practical-data-de-identification/ (accessed Sep. 15, 2021).

[7] F. Inria, "Testing the Robustness of Anonymisation Techniques," 2016.

[8] A. Brasoveanu, M. Moodie, and R. Agrawal, "A Survey of Automatic Contact Tracing Approaches," in *CEUR Workshop Proceedings*, 2020, vol. 2657, pp. 1–9. doi: 10.1145/nnnnnnn.nnnnnnn.

[9] L. Reichert, S. Brack, and B. Scheuermann, "A survey of automatic contact tracing approaches using bluetooth low energy," *ACM Transactions on Computing for Healthcare*, vol. 2, no. 2. Association for Computing Machinery, Mar. 01, 2021. doi: 10.1145/3444847.

[10] "ROBERT: ROBust and privacy-presERving proximity Tracing 1," 2020. [Online]. Available: https://github.com/ROBERT-proximity-tracing

[11] Team TraceTogether, "Policy | BlueTrace," Apr. 09, 2020. https://bluetrace.io/policy/ (accessed Feb. 27, 2022).

[12] J. Bay *et al.*, "BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders," Singapore, Apr. 2020.

[13] S. Vaudenay, "Centralized or Decentralized? The Contact Tracing Dilemma," Lausanne, May 2020. [Online]. Available: https://www.golem.de/news/pepp-pt-streit-beim-corona-app-projekt-2004-147925.html

[14] "Apple and Google partner on COVID-19 contact tracing technology - Apple," *Apple Media Helpline*, Apr. 10, 2020. https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/ (accessed Feb. 27, 2022).

[15] "Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems," Apr. 2020.

[16] B. Sowmiya, V. S. Abhijith, S. Sudersan, R. Sakthi Jaya Sundar, M. Thangavel, and P. Varalakshmi, "A Survey on Security and Privacy Issues in Contact Tracing Application of Covid-19," *SN Computer Science*, vol. 2, no. 3, May 2021, doi: 10.1007/s42979-021-00520-z.

[17] J. S. Warner and R. G. Johnston, "GPS Spoofing Countermeasures".

[18] Y. Gvili, "SECURITY ANALYSIS OF THE COVID-19 CONTACT TRACING SPECIFICATIONS BY APPLE INC. AND GOOGLE INC.," Sep. 2020.

[19] Aaqib Bashir Dar, Auqib Hamid Lone, Saniya Zahoor, Afshan Amin Khan, and Roohie Naaz, "Applicability of Mobile Contact Tracing in FightingPandemic (COVID-19): Issues, Challenges and Solutions," Sep. 2020.

[20] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, "Jamming attacks on wireless networks: A taxonomic survey," *International Journal of Production Economics*, vol. 172. Elsevier, pp. 76–94, Feb. 01, 2016. doi: 10.1016/j.ijpe.2015.11.008.

[21] E. Massé, O. Reich, and E. Simon, "ONE YEAR UNDER COVID-19 CONTACT TRACING APPS: WHAT HAS EUROPE LEARNED? #trackthetrackers," *Civil Liberties Union for Europe e.V*, 2021.

[22] A. Tomaschek, “A Comparison of Contact Tracing Apps From Around the World,” *ProPrivacy*, Jul. 15, 2021. https://proprivacy.com/guides/comparing-contact-tracing-apps-coronavirus-world (accessed Mar. 19, 2022).

[23] “COVID-19 contact tracing apps from around the world - htn,” *Health Tech Newspaper*, May 06, 2020. https://htn.co.uk/2020/05/06/covid-19-contact-tracing-apps-from-around-the-world/ (accessed Mar. 19, 2022).

[24] B. Patel, “Top 11 Healthcare App Ideas to Start a Successful Startup in 2022,” *Space O Technologies*, Aug. 17, 2021. https://www.spaceotechnologies.com/blog/healthcare-app-ideas/ (accessed Mar. 19, 2022).

[25] F. Chiusi, “Digital contact tracing apps: do they actually work? A review of early evidence - AlgorithmWatch,” *Algorithm Watch*, Jul. 08, 2021. https://algorithmwatch.org/en/analysis-digital-contact-tracing-apps-2021/ (accessed Mar. 19, 2022).

[26] G. Fox, T. Clohessy, L. van der Werff, P. Rosati, and T. Lynn, “Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications,” *Computers in Human Behavior*, vol. 121, Aug. 2021, doi: 10.1016/j.chb.2021.106806.

[27] European Commission, “Mobile contact tracing apps in EU Member States | European Commission.” https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en (accessed Mar. 20, 2022).

[28] “AltBeacon - The Open Proximity Beacon.” https://altbeacon.org/ (accessed Jun. 04, 2022).

[29] “Push Notification Software to Improve Customer Engagement - OneSignal.” https://onesignal.com/ (accessed Jun. 04, 2022).

[30] “Error Monitoring & App Stability Management | Bugsnag.” https://www.bugsnag.com/ (accessed Jun. 04, 2022).

[31] “What is OpenTelemetry? | OpenTelemetry.” https://opentelemetry.io/docs/concepts/what-is-opentelemetry/ (accessed Jun. 04, 2022).