St. Cloud State University

The Repository at St. Cloud State

Culminating Projects in Information Assurance

Department of Information Systems

10-2021

Privacy and Security Implications in COVID-19 Tracking/Tracing Apps

Sajjan Shrestha

Follow this and additional works at: https://repository.stcloudstate.edu/msia_etds

Recommended Citation

Shrestha, Sajjan, "Privacy and Security Implications in COVID-19 Tracking/Tracing Apps" (2021). *Culminating Projects in Information Assurance*. 121.
https://repository.stcloudstate.edu/msia_etds/121

This Starred Paper is brought to you for free and open access by the Department of Information Systems at The Repository at St. Cloud State. It has been accepted for inclusion in Culminating Projects in Information Assurance by an authorized administrator of The Repository at St. Cloud State. For more information, please contact tdsteman@stcloudstate.edu.

Privacy and Security Implications in COVID-19 Tracking/Tracing Apps

By Sajjan Shrestha

A starred paper

Submitted to the Graduate Faculty of

St. Cloud State University

In Partial Fulfillment of Requirements

For the Degree of

Master of Science

In Information Assurance

May, 2021

Committee members:
Abdullah Abu Hussein, Chairperson
Jim Chen
Lynn Collen

Abstract

The problem addressed by this research paper is the lack of data security and privacy in COVID-19 tracking and tracing mobile applications. There have been reports of countless COVID-19 tracking and tracing apps leaking data and making use of geo location, which has left users fearful of their data being misused. This research intends to examine and investigate those mobile applications, their features, and their working mechanisms to disclose potential threats to user data. In case the personal user data gets in the hands of people with ill intentions, the data can be misused to commit illegal activities, putting the lives and legal records of users directly in harm. Hence, this is a crucial topic to be studied and solved in the current times. This research paper will firstly be explaining terms like tracking and tracing in order to make the concept of these mobile applications clearer to the readers. Additionally, this research paper will be presenting a list of all the COVID-19 tracking and tracing that have been available and are active around the world, including the USA. Furthermore, this research paper will be presenting cases of COVID-19 tracking and tracing apps that have been found to have violated user privacy and data security. Then, this research paper will be investigating the features of these faulty covid-19 tracking and tracing applications for flaws that result in unauthorized data sharing. After that, this research paper will be making educating recommendations and suggestions to users to prevent unauthorized data sharing and disruption of their data privacy. Lastly, this research paper will be studying multiple researches done on the same topic previously by researchers around the world and will be providing critical review on those research papers published before this one. By performing research on all the previously mentioned topics, this research paper intends to contribute to the process of solving user privacy and data security issues in COVID-19 tracking and tracing applications.

Table of Contents

Page

List of Tables

Table Page

List of figures

Figure Page

Chapter I: Introduction

Introduction

COVID-19 or the Corona Virus, having taken 4,173,058 recorded deaths worldwide, has posed as the most catastrophic pandemic of the decade Worldometer, 2021). On the other hand, the pandemic caused global disruption and an economic devastation to many sectors that have been particularly significant to suffering economies (Zeinalipour-Yazti et al., 2020).

Along with adversities faced by the economic, health, industrial, political, and education sector, personal-data leaks and misuse has been a prime problem faced by technological organizations attempting to track and trace COVID-19 cases with computer and mobile phone applications. The proposed location-based technologies in response to COVID-19 are primarily based on the foundations of mobile commerce, encompassing a wide range of applications that can potentially use proximity details, identity, location data, and other condition information in the provision of value-added services to end-users (Abbas et al., 2020).

Cases have risen where COVID-19 tracking, and tracing apps have threatened the privacy and data security rights of the users. In the process of taking information from the users for the goal of tracking and tracing COVID-19 cases, these applications have failed to comply with the data security and privacy laws, making it harder for the general public to adapt to these applications.

This research paper focuses on this very issue, seeking to discover and address cases of data security failure among covid-19 tracking and tracing apps around the world.

The paper also reflects errors in the methods and outcomes of previous researches on this issue, presenting a critique on previous researches.

Problem Statement

Amidst the Covid-19 pandemic, Covid-19 tracing and tracking apps that utilize patient’s sensitive data to record their health and whereabouts need to keep the data protected and prioritize user privacy to ensure compliance to privacy laws and insure the users from data theft.

Today, too many covid-19 tracking, and tracing apps have been flagged, reported, and discarded for mishandling users’ personal information, while heightening fear of data loss and theft among users. For example, a Norwegian app Smittestopp was suspended because it was uploading live or near-live user locations as GPS coordinates to a central server (Brewster, 2020).

According to Helpnet Security (2020), 85% of COVID-19 tracking apps leak data. Infosecurity-magazine (2020) reports, a Dutch COVID-19 tracking app leaked 200 users’ personal data after collecting it to help the country emerge from lockdown using widespread contact tracing. This app was among 7 apps that was shortlisted by the government for leaking user data. Researchers discovered a flaw in the Qatar Covid-19 app that might have let hackers to access over a million people's national ID numbers and health condition. A researcher uncovered a security flaw in India's app that allowed him to pinpoint who was sick in specific residences (Starks et al., 2020).

Issues like these have delayed the adaptation of COVID-19 tracking and tracing applications among the public, working against the goal of the applications in the first place. Applications need to be able to ensure total data security and privacy when it comes to users’ personal data. Only then, tracking and tracing applications can be used by the general public, contributing to the agenda of the applications to minimize direct contact COVID-19 transmission.

Nature and Significance of the Problem

As this world is struggling to fight the COVID-19 pandemic, governments and corporations are trying their best to come up with technologies and mobile applications that can trace and track human contacts. Encouraged by the White House, much of that pressure to act has focused on Silicon Valley and the tech industry, which has responded with a fragile digital solution (Soltani et al., 2020). Digital contact tracing involves identifying infected individuals and then tracing the people they have been in contact with (Frith et al., 2020).

This way the government and the health agencies would be able to find if someone has been in contact with a person with COVID-19. However, this would require fast public adaptation to the technology and issues like low data security and privacy will only slow down this process, as the public needs a secure system that they can adapt to. And hundreds of scientists and researchers have signed a statement warning "mission creep" could eventually lead to "unprecedented surveillance of society at large" (Kelion, 2020). Therefore, it is crucial to solve the problem of low data security and privacy in COVID-19 tracking and tracing apps because this affects everyone, as everyone might have to use COVID-19 tracking and tracing apps to stay safe in the future. Data, when fallen into wrong hands, can result in important accounts being backed, identity theft, and various other malpractices.

When and if wrong incidents like these take place, the public will be hesitant to adapt to and use the new tracking and tracing apps. This will make the tougher for policymakers to implement their tracking and tracing plans using these Hence, solving this problem is exceedingly important.

Objective of the Study

The research primarily plans to study COVID-19 tracking and tracing applications and find the following information:

1. Find all the COVID-19 tracking and tracing applications that were/are used currently around the world
2. Investigate the COVID-19 tracking and tracing apps that were reported to have leaked user data
3. Research the app features for causes of data security and privacy issues in COVID-19 tracking and tracing apps
4. Analyze previous researches done on the same topic and provide personal views on them.
5. Provide recommendations to protect personal data from being threatened by COVID-19 tracking and tracing apps

Study Questions/Hypotheses

Some questions that the research intends to find answers to are as follows:

i. What are the available COVID-19 tracking and tracing applications?

ii. Which COVID-19 tracking/tracing apps were found to have data privacy and security issues?

iii. What features in the COVID-19 tracking/tracing apps are making the data vulnerable to threats?

iv. What researches have been done on COVID-19 tracking and tracing apps previously?

v. What can you do to make your data more secure and resolve data privacy issues?

Definition of Terms

Apple ID access: Permissions to access Apple iCloud account email address.

Background apps: Permissions to view all the mobile applications that are running in the background on smartphone.

Bluetooth connection/pairing access: Permission to automatically connect to nearby devices via Bluetooth network without user control and share data between the devices.

Camera access: Permissions to access and control the smartphone camera.

Contact information access: Permission to retrieve the phone number of the sim card inserted in the user device.

COVID-19: COVID-19 Stands for Corona Virus Disease 2019, which is a disease caused by a new strain of coronavirus.

Data privacy: Data Privacy describes the practices which ensure that the data shared by customers is only used for its intended purpose.

Data Security: Data security is a set of standards and technologies that protect data from intentional or accidental destruction, modification, or disclosure.

Deploy: Bring into effective action; utilize.

Direct contact transmission: Direct transmission means the transmission of an infectious agent from a reservoir to a susceptible host by direct contact or droplet spread. Direct contact occurs through skin-to-skin contact, kissing, and sexual intercourse. Direct contact also refers to contact with soil or vegetation harboring infectious organisms.

Discard: Get rid of (someone or something) as no longer useful or desirable.

Flag: Mark (an item) for attention or treatment in a specified way.

Full network access: Permission to view what Bluetooth, Wi-Fi, and cellular networks the smartphone is connected to.

Geodata: Computerized geographical Data

Global positioning system (GPS): A space-based radio-navigation system consisting of a constellation of satellites broadcasting navigation signals and a network of ground stations and satellite control stations used for monitoring and control.

GPS: An accurate worldwide navigational and surveying facility based on the reception of signals from an array of orbiting satellites.

Health Information access: Permission to retrieve user fitness data like heart rate, daily footsteps, period cycle in women and so on from mobile applications like Apple Health and Huawei Health.

ID access: Request for government ID number and information like name, address, ID number, date of birth.

Install shortcuts access: Permission to install shortcuts of files and applications in the smartphone storage.

Literature: written works, especially those considered of superior or lasting merit.

Location access: Permission to turn location setting on automatically without user control and connect the device with GPS satellite to track the exact geographical location of the device.

Media access: Permission to access, modify and delete photos, audio, video, and text files.

Mobile Application: A computer program or software designed to run on a mobile device such as a phone, tablet, or watch.

Pandemic: A disease prevalent over the whole world of a whole country.

Phone call access: Permission to make phone calls and access the call contacts and history on the smartphone.

Prevent device from sleeping access: Permission to keep the smartphone running even when the users have preferred settings for the smartphone to shut down or turn off after a certain period of inactivity.

Privacy: the state or condition of being free from being observed or disturbed by other people.

Qualitative: Data that seeks to describe a topic more than measure it. For e.g., opinions, views, and impressions.

Quantitative: Data that can be measured. For e.g., numbers, signals

Run automatically at startup access: Permission to launch the mobile application automatically without user control when the user turns the smartphone on.

Tracing: Measuring the distance between normal individuals and individuals infected by COVID-19.

Tracking: Follow the course of trail of a person infected by COVID-19.

USB Storage access: Permission to access, modify and delete files stored in the smartphone storage.

Vibration access: Permission to control the smartphone vibration settings and modify them.

Wi-Fi access: Permission to turn on/off and connect to Wi-Fi networks through the smartphone automatically without user control.

Summary

Since the COVID-19 pandemic started in early 2020, scientists, governments, and tech companies have introduced numerous tracking and tracing mobile applications to reduce direct contact transmission of the disease. However, the data collected by these applications have left users facing a loss of privacy and insecurity with sharing their personal data. Numerous COVID-19 apps have gotten flagged, discarded, and banned because of privacy law violations. Multiple researches have also been done on the data security issues in COVID-19 tracking and tracing apps.

This research paper intends to firstly, list out the tracking and tracing applications that have been introduced to the public. Then this paper seeks to investigate the apps with data privacy and security issues and look for the exact features of the applications that are causing data security and privacy issues. After dissecting the features and their effect on data security and privacy, the paper seeks to provide solutions and recommendations to resolve data privacy and security issues in the COVID-19 tracking/tracing apps. Lastly, this research paper analyzes previous research papers published on the same topic and provide personal views and recommendations.

Chapter II: Background and review of literature

Introduction

With measures to eradicate contain the Corona Virus disease, IT companies and government around the world have introduced mobile applications that track an individual based on personal information like name, address, phone number and geo location that they agree to share. However, with data sharing, came the issues of lacking data security and data privacy. The mobile applications started employing a variety of methods, including keeping logs of users' Global Positioning System (GPS) location data and asking them to scan Quick Response (QR) codes, which created a fear of being tracked and constantly followed in the application users (Kelion, 2020).

This research paper uses the data and information from articles of Literature related to the problem and each literature article is cited and mentioned in the introduction section, giving the intentions of the research paper a rigid form. The articles mentioned are scholarly articles on COVID-19 tracking/tracing issues and have been verified as a legitimate source of information. Some sources that have contributed data to this research paper are reputed tech blogs that explain and discuss mechanisms of COVID-19 tracking and tracing mobile applications. The section also concisely presents the significance and importance of the chosen articles.

Moreover, the following section in this chapter-literature related to the methodology section lists the literary articles that have contributed to the methodologies of the research paper by providing crucial information like statistics, tables, graphs, and figures for supporting claims made in the paper. These statistics prove that the lack of security and privacy in COVID-19 mobile applications is a growing problem and a massive hindrance in the process of containing the COVID-19 disease. With corporations and governments investing in these tracking and tracing applications to help bring down the growing COVID-19 cases, security and privacy issues need to be addressed before the applications are deployed among the public. Only then the plan to solve the issue of growing COVID-19 cases will start to move ahead towards success.

Lastly, the summary section sums up the chapter, giving the readers a condensed extract of the highlights of the chapter. Although data and statistics are present in the portions mentioned earlier in this section, the summary section gives the readers a quick overview of the claims and conclusions provided by the sections in the chapter.

The aforementioned sections of the chapter build a strong and robust base that the research paper is built on. The contents of this chapter make a clear and comprehensible map of the research paper. As we go further in the research paper, the information and findings are found to be connected and in context with the details mentioned in this chapter.

Background Related to the Problem

According to World health Organization (2020), COVID-19 or the Corona Virus disease is caused by SARS-COV2 and has been the cause of over 1 million recorded fatalities with over 39 million cases worldwide in the year 2020. Claimed to have originated in the wet animal markets in Wuhan City, China, the COVID-19 outbreak infected a massive chunk of the world population in a matter of months, person-to-person transmission being the primary mode of transmission. Then, extensive measures to minimize person-to-person transmission of COVID-19 was enforced to restrict transmission. This is when mobile app companies introduced the COVID-19 tracking and tracing apps as health tools to assist health officials to track down exposures after an infected individual are identified. Using GPS location on phones and personal information for identification, these apps have been able to track and trace COVID-19 patients, however, crucial consumer privacy and data security issues exist with these tracking/tracing apps. This paper discusses these data security and privacy issues in detail in its latter sections.

Data security and privacy refers to the right of an individual to have their personal data like address, phone number, social security number and location confidential.

According to Cliqz.com, in terms of COVID apps, tracking means determining a person’s current location using geodata (GPS), whereas tracing means measuring the distance of phones to record physical contacts between people (Greif, 2020). In other words, tracking constantly transmits an individual’s current location, while tracing records how close has an individual come to a COVID-19 patient physically.

Soon after the governments of different countries deployed COVID-19 tracking and tracing apps, privacy and data security concerns started rising. For example, On March 20, 2020, the Singaporean Ministry of Health released the TraceTogether app for Android and IOS (Cho et al., 2020). The app was found to be providing little to no privacy for infected individuals, as infected individuals were compelled to release their personal data. Information like the person’s name, location, contact number, and health information could be in threat, as a snooper or someone with the authority could misuse it.

To name some COVID-19 tracking and tracing applications, COVID-19 Gov PK (Pakistan), Health Canada (Canada), COVID-19 DXB (Dubai), Covid (Qatar) and Beware Bahrain (Bahrain) are among countless Covid-19 contact tracing applications that governments all around the world have brought into use (Azad et al, 2020). Many of these applications are found to have requested access to location, mobile network, media, prevent from sleeping, camera, microphone, and even device ID. Given that contact tracing and tracking mobile applications are one of the most popular ways of preventing direct contact transmission from COVID, data security and privacy issues need to be examined and resolved.

Data security and privacy could leave people fearful of adapting the new applications, which would dismantle the goal of the governments to stabilize growing COVID-19 cases. This research paper intends to study the information and data security features of apps like TraceTogether and make strategic recommendations to protect the data better.

Literature Related to the Problem

In the Qatar Covid-19 app, researchers found a vulnerability that would've let hackers obtain more than a million people's national ID numbers and health status. In India's tracking app, a researcher discovered a security gap that allowed him to determine who was sick in individual homes. North Dakota conceded in May that its smartphone app, Care19, had been sending user location data to the digital marketing service Foursquare (Starks et al, 2020).

A simulation on one million people found that 80% of smartphone users in the UK (56% of the general population) would need to install a contact-tracing app to suppress the epidemic effectively. A survey run in five countries with more than 6000 potential app users suggested that lower numbers would install a similar app (73.6% of users in the UK, and 67.5–85.5% in France, Germany, Italy, and the USA). In Singapore, the first country to deploy a voluntary contact-tracing app (TraceTogether), launched in March, only an estimated 17% of the population installed the app. After a spike in new cases in April, the city-state introduced a lockdown named ‘circuit breaker’ (Lapolla et al, 2020). Covid-19 tracking, and tracing applications have been a prime approach deployed by governments in past and the future to achieve containment of the COVID-19 disease. However, tracking and tracing applications have failed to secure user data, leaving the government and the users completely fearful of their misuse.

Incidents above prove that the lack of data security and data privacy is a whole issue in its own under the COVID-19 pandemic umbrella, affecting users firstly by inducing fear of data leaks and then by preventing them from adapting to COVID-19 tracking and tracing applications. Besides individuals, this issue has also been a roadblock in the governments’ plans to deploy technological tools like mobile applications to fight the pandemic. Therefore, publishing research papers that dissect the issue of low data security in COVID-19 tracking and tracing applications is very crucial. Lack of research and research papers will leave the public firstly unaware of the issue, and secondly powerless against the issue.

Publishing literature that explains the issue and recommend ways to minimize or eventually remove it will not only help the users adapt to the new COVID-19 tracking and tracing applications, but also help the health agencies smoothly implement their plans to tackle COVID-19 pandemic by using tracking and tracing mobile applications.

Literature Related to the Methodology

To reach its goals, the research paper utilizes information presented by some scholarly researches performed on the exact or similar topics. Researches that have been performed by scholars from the most competent reputable makes a great source of idea, knowledge, and update on the issue in hand. These research literatures are also a great milestone in the process of solving the data security and privacy issue with COVID-19 applications. Some of these literatures are mentioned below.

Firstly, online forums like Cliqz have been cited and reviewed in order to make the readers familiar with the concepts of tracking and tracing and know their differences. An article named – Corona App: What’s the Difference Between Tracking and Tracing has been used to lay out the foundation for this paper, as it explains what is tracking, tracing and how each of these features in a mobile application work to meet their goals and intentions. This will give the research a clear view ahead (Kelion, 2020).

After that, a research paper named- A First Look at Privacy Analysis of COVID-19 Contact Tracing Mobile Applications by Muhammad Ajmal Azad, Junaid Arshad, Syed Muhammad Ali Akmal, Farhan Riaz, Sidrah Abdullah, Muhammad Imran and Farhan Ahmad has been reviewed and cited. This paper does a remarkable job at breaking down how COVID-19 tracking and tracing apps work and what mobile features they make use of while working. This paper explains mobile communication mechanisms like Bluetooth and geo location that COVID-19 applications use to track and trace COVID-19 cases (Azad et al., 2020).

Then, Contract Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs by Hyunghoon Cho, Daphne Ippolito, and Yun William Yu does a great job at describing the privacy rights that consumers have to give up while using COVID-19 tracking and tracing apps (Cho et al., 2020). They use the example of TraceTogether application deployed by the Singaporean government and explain in detail the threats on personal consumer data. However, Contract Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs covers the case of a single COVID-19 tracking/tracing application used by the Singaporean government. Different COVID-19 tracking, and tracing applications might have different features causing the loss of data privacy in various ways. Therefore, more literatures need to be examined and studied in order to reach the heart of this issue.

A Study of the Privacy of COVID-19 Contact Tracing Apps by Haohuang Wen, Qingchuan Zhao, Zhiqiang, Dong Xuan, and Ness Shroff throws light on the lack of privacy on COVID-19 tracing apps by studying 41 total released COVID-19 tracking and tracking applications (Wen et al., 2020). The article also breaks down the types of tracking and tracing and their data requirements. This is a great study in terms of coverage of COVID-19 tracking and tracing applications, as it covers not just 1 but 41 applications in total, giving the readers an idea about the general and individual effects of the features of these COVID-19 tracking/tracing applications.

Furthermore, to back the claims with appropriate and credible statistics on COVID-19 tracking and tracing mobile applications, an article named- Data Privacy Issues in COVID-19 Contact Tracing Apps from the tach blog- Morgan Lewis has been utilized (Dudkewitz et al., 2020). As no claim is complete without a robust base if statistics and numbers, this article has been used as a source of data extracted from a survey of 50 COVID-19 tracking and tracing applications all around the world.

Summary

COVID-19 tracking and tracing applications, although considered an effective tool for locating the whereabouts of COVID-19 patients, have brought about data security and privacy risks that has caused delay in their adaptation by the public. Since it is the age of technology advancement, the introduction of COVID-19 tracking, and tracing apps is a remarkable medium to bring about containment of the disease. However, at what cost?

The application Tracetogether by the Singaporean government, and many others alike have, in efforts to track and trace COVID-19 cases, caused the users’ right to privacy and security by recording crucial entities like the current location, personal contact number, personal address, government identification numbers, birth dates, and age.

Numerous COVID-19 tracking, and tracing applications have been reported to extract sensitive data like location and personal address of users that would allow the mobile application companies to exactly pinpoint the location of an individual. Regardless of the motive of the applications.

Chapter III: Methodology

Introduction

In Chapter III of the research project, the tools utilized in order to carry out this research and get the desired outcomes will be listed. These mentioned tools and techniques, in varying levels, are used for the purpose of finding data, shaping data, and finally presenting the data that ultimately answers the questions asked in the previous chapters of this research paper.

Every research requires a set of technical and non-technical skills that aid in driving the results intended by the research. The choice of these technical and non-technical skills needs to be made carefully as the use of wrong or unfit tools in relation to the desired outcomes of the research. Likewise, this research of COVID-19 tracking, and tracing applications has its own set of these tools that will be mentioned and described in detail in the following parts of this chapter.

In the process of researching the lack of data security and privacy in COVID-19 tracking and tracing applications, firstly, all the COVID-19 tracking, and tracing applications need to be listed out in order to acknowledge the readers about the available options out there. Then, the COVID-19 apps that have been reported to found to have threatened users' privacy and data security need to be filtered out and listed. After that, the defective COVID-19 tracking, and tracing applications are to be examined and those features need to be found that have been causing the lack of data security and privacy. Lastly, some educated recommendations are to be given in order to mitigate and minimize the problem of lacking data security and privacy. Lastly, some previous researches are to be analyzed and their short comings pointed out.

To generate the intended results, the research utilizes the quantitative and qualitative data from several scholarly articles and research papers from legitimate and reported sources.

Design of the Study

To generate the intended results, the research utilizes the quantitative and qualitative data from several scholarly articles and research papers from legitimate and reported sources. The research will undertake both qualitative and quantitative approach to find answers required by the paper.

Qualitative and quantitative and the two natures of approaches used in research, and it is firmly believed that research isn’t complete without being speculated and analyzed by the use of both qualitative and quantitative approaches to bring about a conclusion. Similarly, the use of qualitative results without a measure of the quantitative metrics results in the outcomes being short on logic. Therefore, both qualitative and quantitative approaches are utilized in the research in a manner that they complement their respective outcomes.

For finding answers to questions like the list and number of COVID-19 tracking and tracing applications, number of applications reported for lack of data security and privacy, and location where the applications were deployed, quantitative research will be used. For finding answers to questions like features that cause lack of data security and privacy and recommendations, qualitative research will be exercised.

Data Collection

The research primarily intends to list out the most used COVID-19 tracking and tracing applications. Then it intends to mention the COVID-19 applications that have been flagged or highlighted on News platforms for being a victim of data breaches and leaks. After that, the research intends to look closer into these COVID-19 tracking and tracing applications to find the weak links on the user end that might make them vulnerable to threats. Then, this research intends to make educated and researched suggestions to the app users for keeping their personal data safe and their privacy unthreatened. Lastly this paper intends to find more research done on the topic before it and present their summary, strengths, and weaknesses. Answers to all these questions were researched with the help of different platforms on the internet.

Firstly, the list of COVID-19 tracking, and tracing applications was researched by Google searches, which gave numerous results ranging from research papers, news articles, mobile application developer websites, and government statistics that enlisted COVID-19 tracking and tracing apps deployed in regions all over the world. This greatly helped in building the list of 100 COVID-19 tracking and tracing applications from all around the world.

Secondly, a search of research papers and reputed cybersecurity News platforms like Help Net Security presented information about the COVID-19 tracking and tracing applications that were flagged or highlighted due to threats like data leaks and breaches.

Then, mobile app platforms like Google Play store and Apple App Store, where all the COVID-19 tracking and tracing mobile applications are downloaded from. Google and

Apple are the biggest markets for mobile phones applications, and On April 10, 2020, Google and Apple announced their alliance, stating that they are working together in the "spirit of collaboration" to "allow the use of Bluetooth technology to help governments and health organizations decrease the spread of the virus (Michael et al., 2020). These mobile application platforms have written details about the permissions and access that the mobile applications request once downloaded on smartphones. Depending on the permissions and access, these mobile applications can control or modify files and features in a smartphone. These sources provided the mobile application details that the research intends to uncover.

After that, research papers and scholarly articles written by qualified scholars around the world were analyzed and studied, along with the aforementioned data, to make the suggestions and recommendations to mobile app users in order for them to protect their data and personal information from being accessed, controlled, or modified by the COVID-19 tracking and tracing applications.

Tools and Techniques

Every research needs tools and techniques for analyzing the data and coming up with conclusions that strengthen the research and help meet its goals. Similarly, this research paper also used some tools and techniques that helps in finding the right and reliable information from the internet and extracting it to use it in the paper.

Firstly, in order to make sure that the data that has been extracted is reliable and has a highly credible and reputed source, we use “www.scholar.google.com”, where only research papers from researchers at highly reputed universities are posted. This way we ensure the quality of the information that we use is high.

Secondly, we use specific keywords while searching for the data to ensure that the search results match our needs and can easily be articulated into our research paper. We use keywords like “COVID 19-tracking and tracing”, “data leak and loss of privacy in COVID-19 tracking and tracing”. This allows us to find only the articles that can potentially contribute to our research paper.

To be specific about the goals of this research and the methods to achieve them, the following approaches are used:

Question: What are the available COVID-19 tracking and tracing applications?

Method: The available COVID-19 tracking, and tracing applications are researched by looking for COVID-19 mobile applications list on Google.

Question: Which COVID-19 tracking/tracing apps were found to have data privacy and security issues?

Method: The COVID-19 tracking/tracing applications that were reported to have privacy and security issues, and data leaking issues will be investigated using credible blogs as well as scholarly articles on Google as a source.

Question: What data and information are COVID-19 tracking and tracing applications accessing from user devices?

Method: This will be investigated by looking closely into the features of COVID-19 tracking/tracing applications by either going to their website or searching for data access permissions.

Question: What researches have been done on COVID-19 tracking and tracing apps previously?

Method: The previous researches performed on the similar topic will again be looked for by searching for scholarly articles by google, reading them, and then checking to see if the questions they answer completely contribute to the investigation and resolution of the lack of data privacy and security in COVID-19 tracking/tracing applications.

Question: How can users keep their data safe and protect their privacy from COVID-19 tracking and tracing applications?

Method: Recommendations and advice on making user data more secure in COVID-19 tracking/tracing mobile applications will be researched by studying scholarly articles on Google.

By following the above methods, the questions mentioned previously about the lack of data security and privacy in COVID-19 mobile applications are intended to be answered. Furthermore, News and other forms of media like videos on YouTube will be made use of to mention updates and progresses in the respective subject of the research paper.

Hardware and Software Environment

In order to proceed towards the results of this research paper, a number of software platforms and hardware devices have been utilized.

Below is a list of hardware and software components used during the research:

Hardware:

1. A computer with a memory of above 64GB to save the files required for the research paper

2. Webcam on the computer for video-calling and meeting the research advisor for guidance on the research
3. Hard disk to save the necessary research files for backup

Software:

1. Microsoft Word to type the research paper
2. Google Chrome to search scholarly articles and blog articles on Google
3. Zoom video calling application to meet with the research advisor for guidance on the research paper
4. Zotero to keep track of all the required articles and blogs and cite them
5. Microsoft Project to create a Gant Chart to track the research progress

Summary

Chapter III titled Methodology went into details regarding the methods used to achieve the results as intended by the research paper. It included a thorough description of the nature of the approach – qualitative and quantitative, along with the reasons they were used as a combination. Moreover, this chapter explained the data collection methods that were used in the research paper to find the information required to answer the questions and draw the conclusions in this research paper. Each question was answered using the information collected from varying platforms on the internet like Google Play store, Apple Appstore, Google Scholar, News platforms like Help Net Security and scholarly articles. The significance and the nature of data retrieved from these sources were clearly described in Chapter III. Lastly, the method used for quantitative and qualitative analysis in order to achieve the results were explained in detail in this chapter. The tools inside the methods were clearly highlighted and their outcomes were distinguished to portray their importance in achieving the results in this research paper.

Chapter IV: Data Presentation and Analysis

Introduction

After describing the research topic, research methods, research questions, research timeline, and research structure, the paper has finally reached Chapter IV where the data that has been researched is presented. After following various qualitative as well as quantitative research methods over countless articles, research papers, News portals, and cybersecurity blogs, a huge amount of data has been found and compiled, that helped the paper answer the questions it intends to.

Firstly, the chapter presents answers for the first question with A list of COVID-19 apps used around the world. The list comprises of a 100 COVID-19 tracking and tracing mobile apps that were used by millions of smartphone users around the world in order to be alerted of COVID-19 infection cases nearby.

Secondly, the chapter presents answers to the second question with a short list of COVID-19 tracking and tracing apps that were flagged or highlighted on the news for leaking personal user data or been a victim of data breaches.

Then, this chapter presents answers to the third research question with a detailed description of the access permissions that each COVID-19 tracking, or tracing app asks the users for. This discloses the data in user devices that the applications can access, edit, or delete after the users agree to their terms and conditions. This clarifies ways the mobile applications could threated user privacy.

After the presentation of the aforementioned data, the remaining two questions of this research will be answered in the next section along with a detailed analysis of the data presented in this chapter.

Data Presentation

Following the COVID-19 pandemic in the first half of the year 2020, governments and technology companies from around the world began utilizing the most advanced methods in technology in order to track and trace COVID-19 infection cases. Here is a list of a 100 COVID-19 mobile applications and the region they are published and used in.

Table 1

List of COVID-19 tracking and tracing applications and their region

No.	App Name	Region
1	TraceTogether	Singapore
2	CUIDAR COVID-19	Argentina
3	Stopp Corona	Austria
4	EHTERAZ app	Qatar
5	ABTraceTogether	Canada
6	Care 19	USA
7	Private Kit	USA
8	COVID Control	Maryland, USA
9	Hamagen	Israel
10	Corona Data Donation	Germany

Table 1 (Continued)

11	Stay Home Safe	Hong Kong
12	COVIDsafe	Australia
13	BlueZone	Vietnam
14	CA Notify	California, USA
15	COVIDWISE	USA
16	Guidesafe	Alabama, USA
17	Covid Trace Nevada	Nevada, USA
18	CO Exposure Notifications	Colorado, USA
19	COVID Alert CT	Connecticut, USA
20	DC CAN	DC, USA
21	Guam Covid Alert	Guam
22	AlohaSafe Alert	Hawaii, USA
23	MD Covid Alert	Maryland, USA
24	MI Covid Alert	Michigan, USA
25	COVIDawareMN	Minnesota, USA
26	WI Exposure Notification	Nevada, USA
27	Covid Alert NJ	New Jersey, USA
28	Covid Alert NY	New York, USA
29	SlowCovidNC	North Carolina, USA
30	Care19 Diary	North Dakota, USA

Table 1 (Continued)

31	Care19 Alert	North Dakota, USA
32	Oregon Exposure Notifications*	Oregon, USA
33	Covid Alert PA	Pennsylvania, USA
34	Rastrea el Virus	Puerto Rico, USA
35	Crush Covid RI	Rhode Island, USA
36	South Carolina Safer Together*	South Carolina, USA
37	WA Notify	Washington, USA
38	UT Exposure Notification	Utah, USA
39	BeAware Bahrain	Bahrain
40	ViruSafe	Bulgaria
41	Chinese Health Code System, jiangkangbao	China
42	CoronApp	Columbia
43	CovTracer	Cyprus
44	eRouska	Czech
45	StopCovid	Georgia, USA
46	GH COVID-19 Tracker	Ghana
47	Rakning C-19	Iceland
48	Aarogya Setu	India
49	Sarthak	Indonesia
50	TousAnti Covid	France

Table 1 (Continued)

51	Smittestop	Denmark
52	SwissCovid	Switzerland
53	COCOA	Japan
54	Immuni	France
55	Nepal COVID-19 Surveillance	Nepal
56	Coronavirus UY	Uruguay
57	NICD COVID-19 Case Investigation	South Africa
58	COVA Punjab	Punjab
59	SOS Corona	Mali
60	Bolivia Segura	Bolivia
61	Hamro Swasthya	Nepal
62	Coronavirus – SUS	Brazil
63	NHS Test and Tracing app	UK
64	TraceCORONA	Germany
65	Vietnam Health Declaration	Vietnam
66	CoronaReport	Austria
67	Corona Warn App	Germany
68	StopTheSpread COVID-19	UK
69	Traze	Philippines
70	STOP COVID19 CAT	Catalonia

Table 1 (Continued)

71	CG Covid-19 ePass	India
72	MySejahtera	Malaysia
73	Covid Alert	Canada
74	COVID19 - DXB Smart App	Dubai
75	HOIA	Estonia
76	CareFiji	Fiji
77	Koronavilkku	Finland
78	TousAntiCovid	France
79	Beat Covid Gibraltar	Gibraltar
80	VirusRadar	Hungary
81	Tawakkalna	Saudi Arabia
82	Tabaud	Saudi Arabia
83	Shlonik	Kuwait
84	NZ COVID Tracer	New Zealand
85	E7mi	Tunisia
86	Corona Tracer BD	Bangladesh
87	DOCANDU Covid Checker	Greece
88	NM Notify	New Mexico, USA
89	ASI	Ecuador
90	Guidesafe	Alabama, USA

Table 1 (Continued)

91	COVID Defense	Louisiana, USA
92	Covid Watch Arizona	Arizona, USA
93	Covid Alert DE	Delaware, USA
94	Mass Notify	Massachussets, USA
95	ROBERT	France
96	Blue Care	Louisiana, USA
97	CombatCOVID PBC	Florida, USA
98	COVID Coach	USA
99	VirusMapBR	Brazil
100	Canada COVID-19	Canada

Regardless of the difference between national development in the countries and regions mentioned in the table above, the method of tracking and tracing COVID-19 cases by using mobile applications is seen as a popular one all over the world. This also means that people from all over the world are exposed to mobile applications that track and trace COVID-19 cases, and in case of fraudulent attacks, and weak mobile application security systems, people from all parts of the world are equally at risk of having their privacy.

COVID-19 applications in news for data breach

Since the start of the pandemic and the rise of COVID-19 tracking and tracing mobile applications, countless companies have taken part in the race of publishing the best tracking and tracing mobile application. However, there are also many covid 19 tracking mobile application companies that did not have the best security frameworks in their mobile applications, because of which they became victims of deadly cyber-attacks that resulted in their data being exposed and stolen. This directly threatened the privacy of their users and put them at risk. On the other hand, many app companies themselves did not make customer data privacy their top priority and ended up misusing users' personal data. Covid-19 tracking and tracing mobile applications that were under highlight in media for these negative incidents are mentioned below.

TraceTogether app, Singapore: Launched in March 2020 in Singapore, TraceTogether creators were found to be sharing its users' personal data with the Police Department of the nation for the purpose of criminal investigations, which caused massive opposition and boycotting from its users in Singapore (Han, 2021).

Ehteraz app, Qatar: In May 2020, a serious security vulnerability in Qatar's mandatory contact tracing app Ehteraz that was although found and fixed quickly, could have caused a leak of millions of users' personal data if exploited by attackers (Amnesty International, 2020).

COVIDSafe app, Australia: In November 2020, Australia's spy agencies were caught collecting users' COVID-19 data by government watch dogs. Although the spy agencies disclosed that they were taking steps to ensure compliance and that the user data would be deleted as soon as practicable, this incident caused a loss of users' trust in the COVID-19 app (Whittaker, 2020).

Care19 diary app, North and South Dakota, USA: In May 2020, Care19 diary app popular in South and North Dakota region in the USA was found to be sharing location and health data with a third-party digital marketing company – Foursquare (Fowler, 2020).

Chinese Health Code System – jiangkangbao, China**:** In January 2021, the Chinese government's mandatory Covid-19 app was found to have multiple leaks of users' data like names, addresses, phone numbers and other personal information, causing celebrity personal information to be auctioned on the internet and backlash from the users (Xue, 2021).

COVID-19 tracking/tracing applications and their data access permissions

Each application that is available for users to download have their own website section or section in Apple App Store/Google Playstore that lists out the data and features that the respective application will be accessing or modifying in the users' smartphones. Upon closely speculating each of the COVID-19 mobile application's download page, we found details of the data access permissions that the applications will be accessing or modifying in the smart phones.

The data permissions that the mobile applications request fall among one or more of these permissions below. The meanings behind these access permissions are as follows:

Bluetooth connection/pairing: Permission to automatically connect to nearby devices via Bluetooth network without user control and share data between the devices.

Location: Permission to turn location setting on automatically without user control and connect the device with GPS satellite to track the exact geographical location of the device.

Contact information: Permission to retrieve the phone number of the sim card inserted in the user device.

ID: Request for government ID number and information like name, address, ID number, date of birth.

Apple ID: Permissions to access Apple iCloud account email address.

Health Information: Permission to retrieve user fitness data like heart rate, daily footsteps, period cycle in women and so on from mobile applications like Apple Health and Huawei Health.

Media: Permission to access, modify and delete photos, audio, video, and text files.

USB Storage: Permission to access, modify and delete files stored in the smartphone storage.

Background apps: Permissions to view all the mobile applications that are running in the background on smartphone.

Camera: Permissions to access and control the smartphone camera.

Wi-Fi: Permission to turn on/off and connect to Wi-Fi networks through the smartphone automatically without user control.

Full network access: Permission to view what Bluetooth, Wi-Fi, and cellular networks the smartphone is connected to.

Run automatically at startup: Permission to launch the mobile application automatically without user control when the user turns the smartphone on.

Prevent device from sleeping: Permission to keep the smartphone running even when the users have preferred settings for the smartphone to shut down or turn off after a certain period of inactivity.

Phone call: Permission to make phone calls and access the call contacts and history on the smartphone.

Install shortcuts: Permission to install shortcuts of files and applications in the smartphone storage.

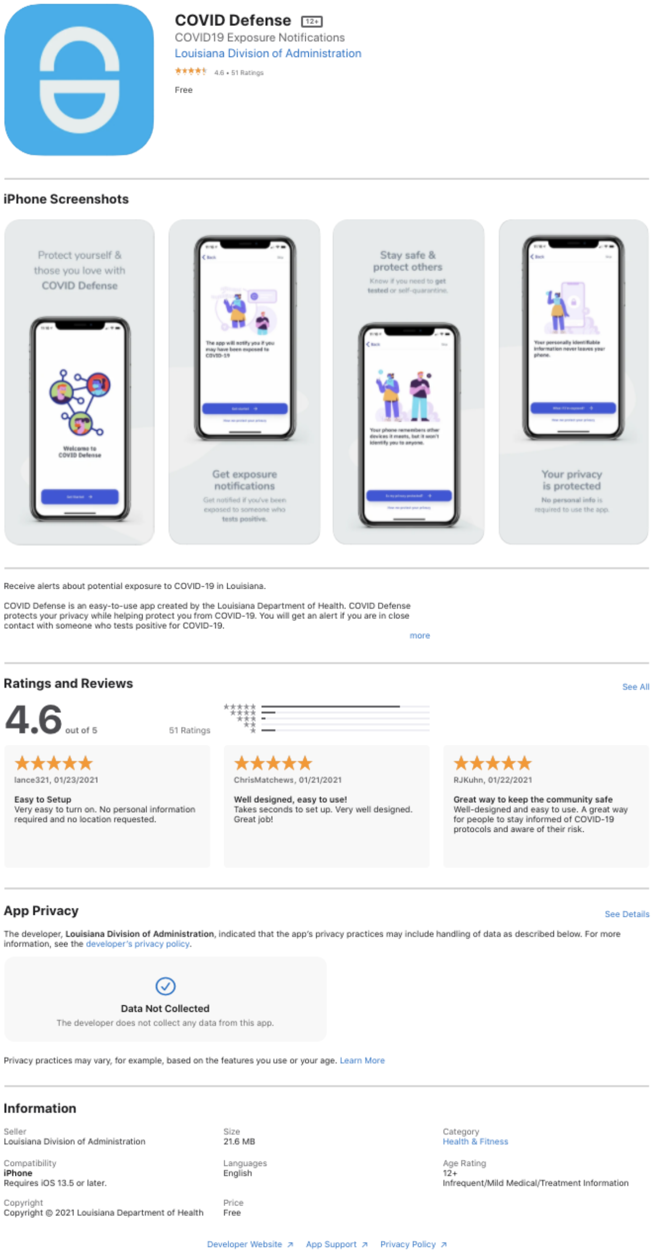
Vibration: Permission to control the smartphone vibration settings and modify them.

Unclear: Either have not disclosed or have written that the application does not access any data in the smartphone.

In order to get the information about what data and phone features the COVID-19 tracking and tracing apps are accessing, users can go to Google Play store, and Apple Appstore pages as shown below to find the information. The area highlighted with red lines is the section where users can check the privacy policies and app permissions for the tracking and tracing mobile applications.

Figure 1

Apple Appstore page for Covid Defense App



COVID Defense 12+

COVID19 Exposure Notifications

Louisiana Division of Administration

★★★★★ 4.6 • 51 Ratings

Free

iPhone Screenshots

Protect yourself & those you love with COVID Defense

Welcome to COVID Defense

The app will notify you if you may have been exposed to COVID-19

Get exposure notifications

Get notified if you've been exposed to someone who tests positive.

Stay safe & protect others

Know if you need to get tested or self-quarantine.

Your phone remembers other devices it meets, but it won't identify you to anyone.

Your personally identifiable information never leaves your phone.

Your privacy is protected

No personal info is required to use the app.

Receive alerts about potential exposure to COVID-19 in Louisiana.

COVID Defense is an easy-to-use app created by the Louisiana Department of Health. COVID Defense protects your privacy while helping protect you from COVID-19. You will get an alert if you are in close contact with someone who tests positive for COVID-19.

more

Ratings and Reviews See All

4.6 out of 5 51 Ratings

★★★★★

lance321, 01/23/2021

Easy to Setup

Very easy to turn on. No personal information required and no location requested.

★★★★★

ChrisMatchews, 01/21/2021

Well designed, easy to use!

Takes seconds to set up. Very well designed. Great job!

★★★★★

RJKuhn, 01/22/2021

Great way to keep the community safe

Well-designed and easy to use. A great way for people to stay informed of COVID-19 protocols and aware of their risk.

App Privacy See Details

The developer, **Louisiana Division of Administration**, indicated that the app's privacy practices may include handling of data as described below. For more information, see the developer's privacy policy.

✓

Data Not Collected

The developer does not collect any data from this app.

Privacy practices may vary, for example, based on the features you use or your age. Learn More

Information

Seller
Louisiana Division of Administration

Size
21.6 MB

Category
Health & Fitness

Compatibility
iPhone
Requires iOS 13.5 or later.

Languages
English

Age Rating
12+
Infrequent/Mild Medical/Treatment Information

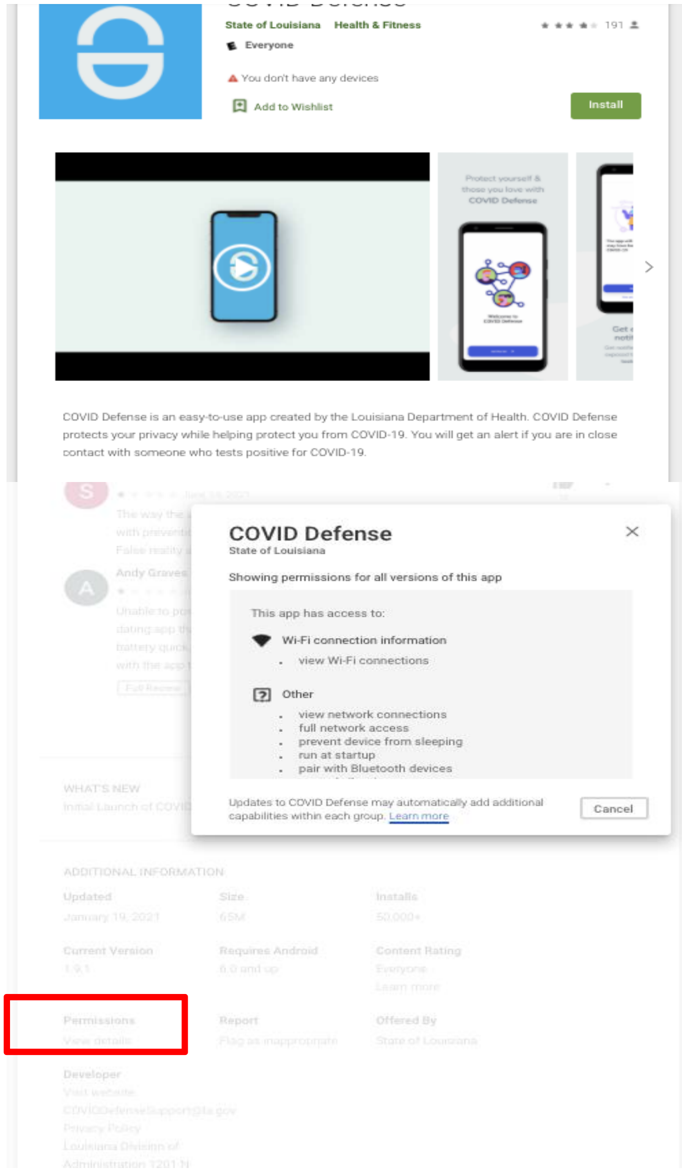
Copyright
Copyright © 2021 Louisiana Department of Health

Price
Free

Developer Website ↗ App Support ↗ Privacy Policy ↗

Figure 2

Google Play store page for Covid Defense App



COVID Defense

State of Louisiana · Health & Fitness · 191

Everyone

You don't have any devices

COVID Defense is an easy-to-use app created by the Louisiana Department of Health. COVID Defense protects your privacy while helping protect you from COVID-19. You will get an alert if you are in close contact with someone who tests positive for COVID-19.

The way the
with preventi
False reality

Andy Graves

Unable to po
dating app th
battery quick
with the app

COVID Defense

State of Louisiana

Showing permissions for all versions of this app

This app has access to:

Wi-Fi connection information
- view Wi-Fi connections

Other
- view network connections
- full network access
- prevent device from sleeping
- run at startup
- pair with Bluetooth devices

Updates to COVID Defense may automatically add additional capabilities within each group. Learn more

WHAT'S NEW

Initial Launch of COVID

ADDITIONAL INFORMATION

Updated	Size	Installs
January 19, 2021	6.5M	50,000+
Current Version	**Requires Android**	**Content Rating**
1.9.1	6.0 and up	Everyone Learn more
Permissions	**Report**	**Offered By**
View details	Flag as inappropriate	State of Louisiana

Developer

Visit website

COVIDDefenseSupport@la.gov

Privacy Policy

Louisiana Division of Administration 1201 N

Table 2

List of COVID-19 tracking and tracing applications and their access permissions

No.	App Name	Data and features access required
1	TraceTogether	Mobile number, ID
2	CUIDAR COVID-19	Apple ID, Health Information, Contact information

Table 2 (Continued)

3	Stopp Corona	Apple ID, Health Information, Contact information
4	EHTERAZ app	Location, contact information, ID
5	ABTraceTogether	Location, contact information
6	Care 19	Unclear
7	Private Kit	Unclear
8	COVID Control	Location, Media, Files, USB storage
9	Hamagen	Background apps, Location, Wi-Fi, Network access, Bluetooth, Alarm, prevent device from sleeping, Run at startup, Vibration
10	Corona Data Donation	ID, address, contact information
11	Stay Home Safe	Camera, Wi-Fi, Bluetooth, Location, Vibration, prevent device from sleeping
12	COVIDsafe	Location Bluetooth, Network access, run at startup, prevent device from sleeping
13	BlueZone	Camera, Wi-Fi, Bluetooth, Location, Vibration, prevent device from sleeping, USB storage, Install shortcuts, Run at startup, Running apps, Media
14	CA Notify	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup

Table 2 (Continued)

15	COVIDWISE	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup
16	Guidesafe	Wi-Fi, Bluetooth pairing, full network access, run automatically at startup
17	Covid Trace Nevada	Running apps, full network access, prevent device from sleep, run automatically at startup, network access
18	CO Exposure Notifications	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup
19	COVID Alert CT	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup
20	DC CAN	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup
21	Guam Covid Alert	Wi-Fi, Bluetooth pairing, full network access, run automatically at startup
22	AlohaSafe Alert	Wi-Fi, Bluetooth pairing, full network access, run automatically at startup
23	MD Covid Alert	Wi-Fi, Bluetooth pairing, full network access, run automatically at startup
24	MI Covid Alert	Wi-Fi, Bluetooth pairing, full network access, run automatically at startup

Table 2 (Continued)

25	COVIDawareMN	Wi-Fi, Bluetooth pairing, full network access, run automatically at startup
26	WI Exposure Notification	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup
27	Covid Alert NJ	Wi-Fi, Buetooth pairing, full network access, run automatically at startup
28	Covid Alert NY	Wi-Fi, Bluetooth pairing, full network access, run automatically at startup
29	SlowCovidNC	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup
30	Care19 Diary	Location, full network access, prevent device from sleeping
31	Care19 Alert	Wi-Fi, Bluetooth pairing, full network access, run automatically at startup
32	Oregon Exposure Notifications*	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup
33	Covid Alert PA	Wi-Fi, Bluetooth pairing, full network access, run automatically at startup
34	Rastrea el Virus	Wi-Fi, Bluetooth pairing, full network access, run automatically at startup

Table 2 (Continued)

35	Crush Covid RI	Location, full network access, prevent device from sleeping
36	South Carolina Safer Together*	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup, control vibration
37	WA Notify	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup, control vibration
38	UT Exposure Notification	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup, control vibration
39	BeAware Bahrain	Running apps, Calendar, Camera, USB storage, full network access, prevent device from sleep, run automatically at startup, network access
40	ViruSafe	Location, full network access, prevent device from sleeping
41	Chinese Health Code System, jiangkangbao	Health information, Contact information, ID
42	CoronApp	Phone call, contacts, ID, Location, Bluetooth access, network access, automatically run at. Startup, alarm

Table 2 (Continued)

43	CovTracer	Wi-Fi, Bluetooth pairing, full network access, run automatically at startup, prevent from sleeping
44	eRouska	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup
45	StopCovid	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup
46	GH COVID-19 Tracker	Camera, Wi-Fi, Bluetooth, Location, Vibration, prevent device from sleeping, USB storage, Install shortcuts, Run at startup, Running apps, Media
47	Rakning C-19	Wi-Fi, Bluetooth pairing, full network access, run automatically at startup
48	Aarogya Setu	Location, Camera, Bluetooth, Network access, run at startup, prevent device from sleeping
49	Sarthak	Camera, Wi-Fi, Bluetooth, Location, Vibration, prevent device from sleeping, USB storage, Install shortcuts, Run at startup, Running apps, Media
50	TousAnti Covid	Camera, Wi-Fi, Bluetooth, Location, Vibration, prevent device from sleeping, USB storage, Install shortcuts, R

Table 2 (Continued)

		un at startup, Running apps, Media
51	Smittestop	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup
52	SwissCovid	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup
53	COCOA	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup
54	Immuni	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup
55	Nepal COVID-19 Surveillance	Location Bluetooth, Network access, run at startup, prevent device from sleeping
56	Coronavirus UY	Wi-Fi, Location, Camera, Phone call, Microphone, Bluetooth, prevent device from sleeping, Media, Network access
57	NICD COVID-19 Case Investigation	Unclear
58	COVA Punjab	Wi-Fi, USB Storage, Location, Camera, Files, ID, Phone call, App history, Bluetooth, prevent device from sleeping, Audio settings, Network access, Vibration

Table 2 (Continued)

59	SOS Corona	Wi-Fi, USB Storage, Location, Camera, Files, ID, Phone call, App history, Bluetooth, prevent device from sleeping, Network access, Vibration, Media
60	Bolivia Segura	ID, Location, Full network access, phone call
61	Hamro Swasthya	Wi-Fi, USB Storage, Location, Camera, Files, ID, Bluetooth, prevent device from sleeping, Network access, Vibration, Media
62	Coronavirus – SUS	Wi-Fi, Bluetooth pairing, full network access, run automatically at startup
63	NHS Test and Tracing app	Health information, Location, Contact information, ID
64	TraceCORONA	Unclear
65	Vietnam Health Declaration	Camera, Wi-Fi, Bluetooth, Location, Vibration, prevent device from sleeping, USB storage, Run at startup, Running apps, Media
66	CoronaReport	Wi-Fi, Bluetooth, Location, Vibration, prevent device from sleeping, USB storage, run at startup, Running apps,

Table 2 (Continued)

		Media
67	Corona Warn App	Camera, Wi-Fi, Bluetooth, Location, Vibration, prevent device from sleeping, run at startup, Running apps, Media
68	StopTheSpread COVID-19	Unclear
69	Traze	Camera, Wi-Fi, Bluetooth, Location, Vibration, prevent device from sleeping, run at startup, Running apps, Media
70	STOP COVID19 CAT	Location Bluetooth, Network access, run at startup, prevent device from sleeping
71	CG Covid-19 ePass	Camera, Wi-Fi, Bluetooth, Location, Vibration, prevent device from sleeping, run at startup, Running apps, Media, USB Storage
72	MySejahtera	Camera, Phone call, Wi-Fi, Bluetooth, Location, Vibration, prevent device from sleeping, Run at startup, Running apps, Media, USB Storage

Table 2 (Continued)

73	Covid Alert	Camera, Wi-Fi, Bluetooth, Location, Vibration, prevent device from sleeping, run at startup, Running apps, Media, USB Storage
74	COVID19 – DXB Smart App	Camera, Wi-Fi, Bluetooth, Location, Vibration, Calendar, Microphone, prevent device from sleeping, Run at startup, Running apps, Media, USB Storage
75	HOIA	Wi-Fi, Buetooth pairing, full network access, run automatically at startup
76	CareFiji	Location Bluetooth, Network access, run at startup, prevent device from sleeping
77	Koronavilkku	Bluetooth, prevent device from sleeping, vibration
78	TousAntiCovid	Camera, Wi-Fi, Network access, Bluetooth, run at startup, vibration, prevent device from sleeping
79	Beat Covid Gibraltar	Wi-Fi, Bluetooth pairing, full network access, run automatically at startup
80	VirusRadar	Location, full network access, prevent device from sleeping, Bluetooth access
81	Tawakkalna	Camera, Files, Media, Location, Bluetooth, run at startup, Network access, Vibration

Table 2 (Continued)

82	Tabaud	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup, control vibration
83	Shlonik	Wi-Fi, USB Storage, Location, Camera, Files, ID, Phone call, App history, Microphone, Bluetooth, Prevent device from sleeping, Audio settings, Network access, Vibration
84	NZ COVID Tracer	Camera, Wi-Fi, Network access, Bluetooth, run at startup, vibration, prevent device from sleeping
85	E7mi	Location, Phone call, Bluetooth, run at startup, prevent device from sleeping, network access
86	Corona Tracer BD	Location, Phone call, Device ID, ID, Bluetooth, run at startup, prevent device from sleeping, network access
87	DOCANDU Covid Checker	Location, USB storage, Media
88	NM Notify	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup, control vibration

Table 2 (Continued)

89	ASI	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup, control vibration
90	Guidesafe	Wi-Fi, Bluetooth pairing, full network access, run automatically at startup
91	COVID Defense	Wi-Fi, Bluetooth pairing, full network access, run automatically at startup
92	Covid Watch Arizona	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup
93	Covid Alert DE	Wi-Fi, Bluetooth pairing, full network access, run automatically at startup
94	Mass Notify	Bluetooth pairing, full network access, prevent device from sleeping, run automatically at startup, control vibration
95	ROBERT	Bluetooth, prevent device from sleeping, vibration
96	Blue Care	Location, running apps
97	CombatCOVID PBC	Location, full network access, prevent device from sleeping, Bluetooth access
98	COVID Coach	Contacts, Microphone, Storage USB, Media, Files, Camera, Wi-Fi, Bluetooth, Run at startup, Prevent device from sleeping

Table 2 (Continued)

99	VirusMapBR	ID, Health information, Bluetooth, Location, Wi-Fi, Data usage, Media
100	Canada COVID-19	Location, Health information, Search history, ID, Bluetooth, Data usage, Network access

The data permission accesses for the COVID-19 mobile applications give you an idea about what data you are potentially putting at risk when you install the applications. Hence, it is crucial to check their app page for these permissions to be on the safe side and not risk data and information in your smartphones that could be used by individuals or organizations with ill intentions to leak, modify, delete, or steal.

Other research done on data privacy in COVID-19 tracking and tracing apps

A First Look at Privacy Analysis of COVID-19 Contact Tracing Mobile Applications by Muhammad Ajmal Azad, Junaid Arshad, Syed Muhammad Ali Akmal, Farhan Riaz, Sidrah Abdullah, Muhammad Imran and Farhan Ahmad does a remarkable job at breaking down how COVID-19 tracking and tracing apps work and what mobile features they make use of while working (Azad et al., 2020). This paper explains mobile communication mechanisms like Bluetooth and geo location that COVID-19 applications use to track and trace COVID-19 cases. However, only 13 mobile applications have been examined for their working mechanisms, while there are over 100 mobile applications that access different data from users' phones. Therefore, more mobile applications need to be studied to come to strong conclusions regarding data privacy in COVID-19 mobile applications.

Contract Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs by Hyunghoon Cho, Daphne Ippolito, and Yun William Yu does a great job at describing the privacy rights that consumers have to give up while using COVID-19 tracking and tracing apps (Cho et al., 2020). They use the example of TraceTogether application deployed by the Singaporean government and explain in detail the threats on personal consumer data. However, Contract Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs covers the case of a single COVID-19 tracking/tracing application used by the Singaporean government. Different COVID-19 tracking, and tracing applications might have different features causing the loss of data privacy in various ways. Therefore, more COVID-19 tracking and tracing mobile applications need to be examined and studied in order to reach the heart of this issue.

A Study of the Privacy of COVID-19 Contact Tracing Apps by Haohuang Wen, Qingchuan Zhao, Zhiqiang, Dong Xuan, and Ness Shroff focuses on the lack of privacy on COVID-19 tracing apps by studying 41 total released COVID-19 tracking and tracking applications (Wen et al., 2020). The article also breaks down the types of tracking and tracing and their data requirements. This is a great study in terms of coverage of COVID-19 tracking and tracing applications, as it covers not just 1 but 41 applications in total, giving the readers an idea about the general and individual effects of the features of these COVID-19 tracking/tracing applications.

Data Analysis

In the previous section of this chapter, the data and information that was retrieved from numerous sources concerning cybersecurity and COVID-19 tracking and tracing applications was presented. The data showed the list of COVID-19 applications, their regions of usage, and the data permissions that they ask for to the users who use those applications. In the Data Analysis section, that information and data from the previous section are analyzed and some statistical calculations performed on them to deduce what they mean in detail. A table that enumerates the number of mobile applications and the access to features they request has been provided below.

Table 3

Permission accesses and the number of applications

SN	Feature	Number of mobile applications
1	**Bluetooth connection/pairing**	78
2	**Location tracking**	42
3	**Contact information**	10
4	**ID**	14
5	**Apple ID**	2
6	**Health Information**	6
7	**Media**	20

Summary

This chapter presented the data and information regarding COVID-19 tracking and tracing applications that were researched and speculated for the features accesses they request. COVID-19 tracking, and tracing applications request accesses for Bluetooth connection/pairing Location tracking, contact information, ID, Apple ID, Health Information, Media, USB Storage, Background apps, Camera, Wi-Fi connection, Full network access, run automatically at startup, prevent device from sleeping, Phone call, install shortcuts, and Vibration depending on which one you download. Once the users grant the access to these applications, they allow the application company to manipulate the respective features on your phone and use the data retrieved from the features. Some of the features allow access to very personal and sensitive information like health information, address, government ID, and location, which in wrong hands, could be misused to a dangerous extent.

Chapter V: Results, Conclusion, and Recommendations

Introduction

Thus far in this research paper, information and data relating to COVID-19 tracking and tracing mobile applications from all around the world and listed out their region, and the phone feature accesses they request the user before they can be used. Moreover, we went a step ahead and analyzed the feature accesses that most mobile applications request and least and presented this information in a table. All the data research, tabulation, and analysis will be playing a huge role in building the results, conclusion, and recommendations. The results, conclusion and recommendations will be presented in this chapter.

The results section will have the findings that we mentioned in the previous sections in a concise manner for the purpose of a quick overview. This section will help the readers to follow through on the researched information and the conclusions that are drawn from them. The conclusion section will have finally answer questions asked in the research paper in the beginning with the help of the researched data and their analysis. Lastly the recommendations section will have educated suggestions to users who download the COVID-19 tracking and tracing applications in order to protect their privacy and sensitive data

Conclusion

The data and research findings presented in the previous chapters draw a clear picture of the reality of COVID-19 tracking and tracing mobile applications, in terms of the phone features and data that they request to access. Especially because mobile phones have become a crucial part of people’s daily lives, it is riskier than ever before to allow these tracking and tracing applications to access the users’ phone features and personal data. Moreover, access to network features like Bluetooth connections and location tracking, can allow attackers to locate and control users’ mobile phones to perform various malicious tasks by making use of user data and phoner features without the consent or knowledge of the users. This will not only invade the users’ privacy but also cause the users to be victims of various criminal activities. Therefore, it is crucial for users to thoroughly go through the terms of agreement of the mobile applications before downloading and accepting the terms of COVID-19 tracking and tracing mobile applications in order to get a good idea about what they are signing up for. This will not only protect users’ data and privacy but will also keep them out of potential criminal activities that attackers might perform using the users’ mobile devices and data.

Recommendations

Mobile phones have become a big part of our lives today. Especially during the COVID-19 pandemic, mobile applications like tracking applications as well as other social media applications are being used in a way higher magnitude as a result of increased phone time. Although COVID-19 tracking and tracing mobile applications were designed and created to bring a solution into the pandemic by tracking exact locations and whereabouts of COVID-19 patients and warning others who don’t have the infection, user privacy might greatly be at stake. Hence, after studying the data and phone features access that the mobile applications request, here are some recommendations that might help one preserve their privacy:

1. Downloading mobile applications from third party stores or website that do not clearly mention the data access requests needs to be avoided at all cost.
2. Mobile applications or companies need to be researched before downloading and using the applications in order to avoid being victims of any negative events or incidents like recent data breaches in the application company.
3. Mobile application privacy policy in the application download store (Google Play store, Apple App store) needs to be checked and their terms of agreement and data access requests need to be read through carefully before downloading the application.
4. Being mindful of phone features like Bluetooth and location and check to see that they are turned off when not necessary is vital.
5. Phone application settings need to be checked and managed carefully in order to make sure usage of features like Bluetooth and location are turned off for unnecessary applications.
6. Smartphones need to be locked with passwords or other authentication methods like Face ID and Touch ID in order to prevent potential unauthorized application downloads.
7. Malicious links in spam emails and websites need to be deleted or closed right away, in order to prevent automatic download of mobile applications into the smartphone.

8. Being mindful of letting people use a personal smartphone is necessary in order to avoid unauthorized mobile application downloads.
9. Being cautious while selecting preferences on mobile application access request popups especially in Apple devices that repeatedly ask at certain intervals for permissions to device Location is important.
10. Educating people who own smartphones about data and privacy protection practices in order to avoid accidents that threaten user privacy is a must.
11. Promote laws on national level that prohibit the use of consumer data for unauthorized operations,

By following the above steps and just being generally cautious about what you download in your smartphone and allow access to data, you can protect your data and privacy and avoid being victims of incidents like data breaches and leaks.

References

8*5% of COVID-19 tracking apps leak data.* (2020, September 30). Help Net Security. Retrieved November 12, 2020, from https://www.helpnetsecurity.com/2020/09/30/covid-19-tracking-apps-leak-data/

Abbas, R., & Michael, K. (2020). COVID-19 Contact Trace App Deployments: Learnings from Australia and Singapore. *IEEE Consumer Electronics Magazine*, *9*(5), 65–70. https://doi.org/10.1109/MCE.2020.3002490

Amnesty International. (2020, May 26). Contact tracing app security flaw exposed sensitive personal details of more than one million. Retrieved July 18, 2021, from https://www.amnesty.org/en/latest/news/2020/05/qatar-covid19-contact-tracing-app-security-flaw/

Azad, M. A., Arshad, J., Akmal, S. M. A., Riaz, F., Abdullah, S., Imran, M., & Ahmad, F. (2020). A First Look at Privacy Analysis of COVID-19 Contact Tracing Mobile Applications. IEEE Internet of Things Journal, 8(21), 15796-15806. https://doi.org/10.1109/JIOT.2020.3024180

Brewster, T. *COVID-19 Tracking Apps 'A Privacy Trash Fire' As Norway Nixes Its Own*. (2020, June 16). Forbes. Retrieved July 25, 2021, from https://www.forbes.com/sites/thomasbrewster/2020/06/16/covid-19-tracking-apps-a-privacy-trash-fire-as-norway-nixes-its-own/

Cho, H., Ippolito, D., & Yu, Y. W. (2020). Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs. *https://arxiv.org/abs/2003.11511*

Dudkewitz, M.O., Pierides, M., & Parks, G. T. (2020, September 3). *Data Privacy Issues in COVID-19 Contact Tracing Apps.* Lexology. Retrieved October 5, 2020, from https://www.lexology.com/library/detail.aspx?g=5f45b116-9287-4c5d-9974-849aafcbe106

Fowler, G.A. *One of the first contact-tracing apps violates its own privacy policy.* (2020, May 21). Washington Post. Retrieved July 18, 2021, from https://www.washingtonpost.com/technology/2020/05/21/care19-dakota-privacy-coronavirus/

Frith, J., & Saker, M. (2020). It Is All About Location: Smartphones and Tracking the Spread of COVID-19*. Social Media* + *Society*, *6*(3), 1-4. https://doi.org/10.1177/2056305120948257

Greif, B. (2020, April 29). *Corona App: What's the Difference Between Tracking and Tracing?* Cliqz. https://cliqz.com/en/magazine/corona-app-whats-the-difference-between-tracking-and-tracing

Han, K. (2021, January 11). *Broken promises: How Singapore lost trust on contact tracing privacy*. MIT Technology Review. Retrieved July 18, 2021, from https://www.technologyreview.com/2021/01/11/1016004/singapore-tracetogether-contact-tracing-police/

Kelion, L. (2020, April 20). *Coronavirus: Why are there doubts over contact-tracing apps?* BBC News. Retrieved July 18,2021, from https://www.bbc.com/news/technology-52353720

Lapolla, P., & Lee, R. (2020). Privacy versus safety in contact-tracing apps for coronavirus disease 2019. *Digital Health*, 6, 1-2. https://doi.org/10.1177/2055207620941673

Michael, K., & Abbas, R. (2020). Behind COVID-19 Contact Trace Apps: The Google–Apple Partnership. *IEEE Consumer Electronics Magazine*, *9*(5), 71–76. https://doi.org/10.1109/MCE.2020.3002492

Muncaster, P. (2020, April 21). *#COVID19 Tracing App Leaks User Data*. Infosecurity Magazine. Retrieved July 18, 2021, from https://www.infosecurity-magazine.com:443/news/covid19-tracing-app-leaks-user/

Soltani, A., Calo, R., & Bergstrom, C. (2020, April 27). *Contact-tracing apps are not a solution to the COVID-19 crisis*. Brookings TechStream. Retrieved July 18, 2021, from https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/

Starks, T. & Cerulus, L. (2020, July 6). *Early Covid-19 tracking apps easy prey for hackers, and it might get worse before it gets better*. POLITICO. Retrieved July 25, 2021, from https://www.politico.com/news/2020/07/06/coronavirus-tracking-app-hacking-348601

Wen, H., Zhao, Q., Lin, Z., Xuan, D., & Shroff, N. (2020). A Study of the Privacy of COVID-19 Contact Tracing Apps. *Security and Privacy in Communication Networks. 335*, 297–317. https://doi.org/10.1007/978-3-030-63086-7_17

Whittaker, Z. (2020, November 24). *Australia's spy agencies caught collecting COVID-19 app data.* TechCrunch. Retrieved July 18, 2021, from https://techcrunch.com/2020/11/24/australia-spy-agencies-covid-19-app-data/?guccounter=1

World Health Organization. *Coronavirus disease (COVID-19) Situation Report - 174* (2020, July 12). Retrieved November 12, 2020, from https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200712-covid-19-sitrep-174.pdf?sfvrsn=5d1c1b2c_2

Worldometer. *COVID Live Update: 194,713,264 Cases and 4,173,058 Deaths.* (2021, July 25) Retrieved July 25, 2021, from https://www.worldometers.info/coronavirus/?utm_campaign=homeAdvegas1?%22

Xue, J. (2021, January 11). *CHINA VOICES | Who's at fault in celebrity health code hack?* TechNode. Retrieved July 18,2021, from http://technode.com/2021/01/11/whos-at-fault-in-celebrity-health-code-hack/

Zeinalipour-Yazti, D., & Claramunt, C. (2020). COVID-19 Mobile Contact Tracing Apps (MCTA): A Digital Vaccine or a Privacy Demolition? *2020 21st IEEE International Conference on Mobile Data Management (MDM),* 1–4. https://doi.org/10.1109/MDM48529.2020.00020