Covid-19 Contact Tracing Privacy Concerns and Mitigation

Tao Jiang(20004769)

158.738 Implementation and Management of Systems SecurityDate

Abstract

There has been ongoing development of contract tracing apps being rolled out to help governments combat the spread of Covid-19. Primarily, these Covid-19 tracing apps are being developed to do well in society. However, there have been privacy concerns related to their use. This report discovered that the contact tracing apps subject its users to having their data mined by entities, private data exposed, and exposure to blackmail and extortion from hackers and other malicious groups. The report suggests that transparency in terms of the type of data collected will allow the user to understand the information being collected by these apps. Similarly, the report suggested that the collected data should be minimized as much as possible, and the contact tracing should also end as soon as Covid-19 ends. A future direction for contact tracing was also identified to be the integration of Artificial Intelligence systems to the tracing software to boost security and increase its efficiency.

Keywords: Covid-19, tracing apps, privacy concerns, security

**1.0 Introduction**

Currently, the whole world is finally united in the pursuit of one common goal: eliminating Covid-19. This strain of the virus was first recorded in China’s Wuhan region in 2019 after a fatality due to a mysterious disease was reported (Veloso & Ziviani, 2020). As such, the virus has spread across the globe, with a current standing of 30,675,675 infections and 954,517 deaths (WHO, 2020). The spread of the dubbed 21st-century pandemic has seen many public and private entities investing in infection prevention measures. The primary prevention measure put in place by governments was social distancing; however, it is hard to control the social nature of humans.

People worldwide have been violating the measures put in place by governments in terms of social distancing. This violation has spurred the development of proximity tracing, otherwise known as contact tracing. This new program is aimed at the monitoring of user movements across different locations. These movement patterns are crucial to the monitoring of infections of Covid-19 from one person to another. According to Iacobucci (2020), the contact tracing program was developed to allow for easy identification of persons who may have come in contact with carriers of the virus.

**2.0 Methodology**

There have been powerful digital technologies inventions ranging from contact tracing applications, Closed Circuit Televisions, credit card history to facial recognition. These digital technologies collectively serve to minimize the spread of Covid-19 through early identification of contacts that may have been in contact with positive parties. For this report, emphasis will be placed on contact tracing applications. The report will analyze how this program has been developed and positioned to minimize the spread of Covid-19. The report will focus on the privacy concerns that have been raised considering the use of these applications.

The report will be written based on the information published by accredited scholars in competent journals. These journals will be analyzed to understand better the basis of the concerns being raised by citizens about the program violating their privacy rights. A critical review of published literature materials will serve as points of reference to arguments enclosed herein and form the pillar for the identified privacy concerns. Lastly, the report will critically analyze the findings of different authors and, in so doing, suggest possible mitigation measures that have or can be implemented to ensure that contact tracing does not subject its users to unnecessary exposure.

**2.1 How Contact Tracing Works**

According to Martinez, Wieten, Magnus, and Cho (2020), contact tracing program works via Bluetooth technologies integrated into smartphones. The figure below summarizes a contact tracing system's operation from the point of contact to the point of action. Starting with the users, persons A and B have contact tracing packets installed on their phones. The packets trigger a continuous broadcast of unique identifiers that other phones can pick up whenever they are within proximity. Let us assume that person A has the Covid-19 virus for this illustration, and person B does not.

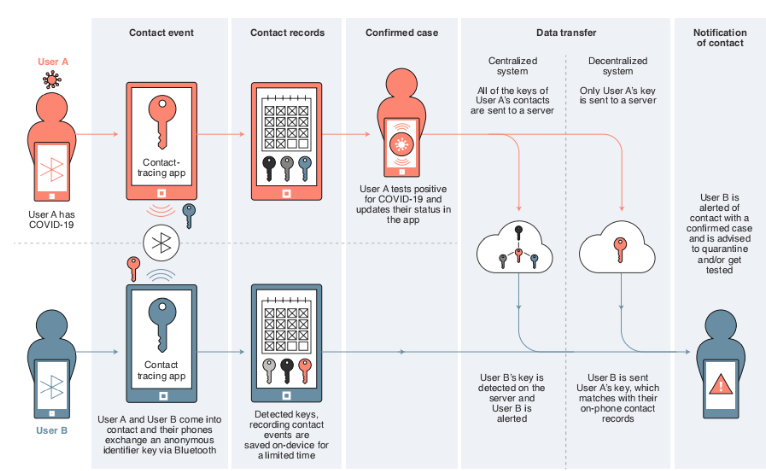


Figure 1: Covid-19 contact tracing app for Bluetooth devices. Source: (Martinez et al., 2020).

As shown in the figure, when person B comes close to person A, both their phones will detect the other's proximity. If the proximity remains constant for a considerable amount of time, the two devices exchange identifier keys via Bluetooth. According to Martinez et al. (2020), the proximity being detected is within a radius of 2 meters. After the exchange of identifier keys occurs, each smartphone temporarily stores the Remote Proximity Identifier key can later be transmitted to the databases run by the contact tracing entities.

When person A has the Covid-19 virus and tests positive for Covid-19 antibodies, they can update their database status as positive. In some cases, public health officers are responsible for posting positive keys on the database to avoid users from falsely representing themselves as negative (Wilson, Warrier & Rathish, 2020). Once the positive status is in the database, it triggers all the identifier keys collected by person A’s phone. Analysis of the keys on the database will point to person B’s interaction with person A, and thus person B is advised to quarantine themselves until they get tested. Alternatively, the identifier key of person A can be posted in a Covid-19 positive database, and other users can use it to check if they came in contact with person A.

**2.2 Contact Tracing Apps currently in use**

The list below summarizes the available contact tracing apps by listing one example of each contact tracing app category. There are three categories, namely; centralized, decentralized, and hybrid architecture.

1. **Trace Together**

Trace Together contact tracing app was developed by Singapore's government to control the spread of the virus within its boundaries. This app consists of a voluntary sign-in option where people can choose whether to adopt it or not. Trace together is based on centralized database architecture.

1. **Apple and Google Exposure Notification**

Google and Apple developed a contact tracing API through collaborative action. Their system is based on a decentralized database system where identifier keys of positive patients are posted in public databases, and individuals can cross-check their interactions.

1. **ConTra Corona**

The tracing app was developed by German researchers to provide security solutions to the previous two categories. It is a hybrid database architecture that combines the centralized server for analysis and decentralized for notification of suspected infections.

**3.0 Privacy Concerns**

1. **Lack of Consent**

Primarily, an individual’s consent is required for any mobile application capable of tracking their real-time interactions with other people and movements. The Covid-19 contact tracing applications need to be bound by the same principle to prevent personal privacy invasion. Some governments like Singapore have respected this human right to privacy and provided voluntary opt-in options for its contact tracing app named Trace Together (Rowe, 2020). However, some countries like China have considered these voluntary options as a challenge on its own.

According to Dropkin (2020), the uptake of the Singaporean Trace Together Covid-19 digital application has been significantly low due to the individual’s concern for their privacy. Acting on this information, some governments have mandated using the contact tracing apps, with some going as far as automatically installing the packets on individual’s phones via over-the-air system updates (Ponce, 2020). This intrusion takes away an individual’s right to privacy of the data stored on their phones and other connected activities. Moreover, some surveillance apps do not come with the option to turn on or off, meaning that the individual is forced into constant surveillance without their informed consent (Fahey & Hino, 2020).

1. **Data Mining**

According to Fahey and Hino (2020), the proximity contact tracing apps being rolled out by the governments allow them to mine user data in terms of location history and movement habits. This mining of user data violates an individual’s privacy by placing real-time tracking on citizens. Contact tracing apps installed in people’s phones tend to be used to collect more than they were primarily meant to do. It means that there is no way of knowing what is collected by governmental intelligence agencies, even though the government promises to collect only Covid-19 related information (Rowe, 2020).

Similarly, the collected information from our Bluetooth encounters with other people can be analyzed on a geographical map to pin-point our locations (Van & Ruijter, 2020). Many organizations tasked with contact tracing have promised to avoid location exposure of individuals and, thus, Bluetooth technology's preference over Geographical Positioning Systems (GPS). However, the movement patterns recorded by Bluetooth in terms of keys can be effectively manipulated by other parties to analyze behavioral patterns based on where we frequently go to and our day-to-day contacts (Oswald & Grace, 2020). This concern shows that any individual during this Covid-19 situation is like a specimen being watched by the government. The 24-hour observation breaks our privacy rights and keeps us exposed to both the government and malicious third parties.

1. **Exposure to malicious entities**

As shown earlier, the Covid-19 contact tracing apps work primarily through the constant broadcasting of Bluetooth signals that other phones can detect and trigger an exchange information command if within proximity for a considerable amount of time. Taking Singapore's Trace Together app, the logs collected during interaction include the user's contact information, which is intended to contact them in case of infection (Gorji et al., 2020). On the other hand, Google and Apple tracking apps provide a public database of infected people's Bluetooth keys. The published information could be collected and used by users for cross-checking if they contact the infected people (Frith & Saker, 2020). In both these cases, the users' phones transmit the logs in the form of Rolling Proximity Identifiers (RPIDs).

The installation of the contact tracing apps on our phones and the connected broadcasting of Rolling Proximity Identifiers (RPIDs) can serve as an avenue for attack from malicious entities. According to (Rowe, 2020), fake Bluetooth towers can be placed on neighborhoods to hijack the Rolling Proximity Identifiers (RPIDs) during a broadcast. This fake towers can be used to mimic the signals broadcasted by the tracing apps. Doing so convinces the victim’s phones to transmit private information as it installs malicious apps that can steal data (Yasaka, Lehrich & Sahyouni, 2020). The hijacked Rolling Proximity Identifiers (RPIDs) can be maliciously used to subject individuals to endless tailored advertisements and scam calls aimed at their particular geographical locations.

1. **Extortion and Blackmail**

Covid-19, similar to HIV and AIDS, comes with social stigma through the allegations of infecting others. As a result of this, it is understandable why some people would not wish to have their positive tests for Covid-19 to be exposed to the public. Primarily, the contact tracing apps do not publish the positive person's identity but instead posts their identifier Bluetooth RPID keys (Bengio et al., 2020). However, according to Li and Guo (2020), the RPIDs can be manipulated by hackers in combination with face recognition and geo-positioning technologies to exactly pin-point the infected person. An example by Frith & Saker (2020), shows that if person A, B, and C are infected after coming into contact with person D then the data of person A, B, and C can be triangulated to estimate the location of the person D. The data can then be refined through face recognition and credit card tracing to identify the person..

The collected information in terms of the infected people's identity can then be used by hackers to blackmail and extort money from the victims with threats of having their information posted online. According to (Janda et al., 2020), there is the possibility of infected people retaliating against their would-be infectors due to the danger of getting infected. As a result, it becomes easy to manipulate and extort the parties responsible for their infection since they would readily pay anything to avoid being subjected to a witch hunt. Similarly, there have been cases of people in South Korea being accused of infidelity and sex work based on the contact tracing apps (Ryan, 2020). This flaw in the contact tracing app has subjected people to exposure of private information such as contact details like emails and phone numbers and residence and work-address details.

1. **Identity theft**

Hackers and other malicious third parties can manipulate Rolling Proximity Identifiers (RPIDs) and mimic false broadcasts to target smartphones. The mimicked broadcasts can take the form of virus-infected data packets, which can be infected as an identifier from a Bluetooth encounter with another user. Once inside the user’s phone, the injected virus can then create vulnerabilities in the host phone that hackers can later manipulate to collect and continuously transmit the user’s data. According to Bengio et al., (2020), unsecured or vulnerable contact tracing apps can pave the way for hackers to siphon information right from the RPIDs or inject their payloads through the creation of fake Bluetooth hotspots within socially frequented areas.

The payloads can be 'listeners,' which can then analyze and record the victim's every interaction. The result of this listening and recording is usually a data map showing all the victim's movements and exposing private information such as credit card pin and all digital banking passwords. Hackers and other malicious parties can effectively use this information to represent themselves as the user falsely. In this case, identity theft is usually done for criminal intent, such as fraudulently acquiring funds or property under the pretext of being the victim of identity theft. Therefore, despite the efficacy of the Covid-19 contact tracing application, we might be avoiding catching the virus at the expense of some of us falling prey to cyber-crimes that could result in loss of data as well as funds.

**4.0 Mitigation Measures**

1. **Introduction of Voluntary participation**

There have been ongoing concerns about the lack of voluntary participation of users in the Covid-19 contact tracing program. As shown earlier, some governments have mandated using these applications to manage and eliminate the Covid-19 virus's spread within borders. According to Yazti and Claramunt (2020), the best solution to this problem is introducing voluntary participation options within the app. The solution is further rooted in the idea that the people will gladly use the app if they feel like they have the final say in choosing when and how to use it.

Starting with installation, the government should not mandate it but rather encourage its citizens to adopt the program since it serves their safety interests concerning Covid-19. Moreover, once installed, the user should reserve the rights and ability to turn the app ON and OFF at will. This capacity will enable them to switch them off at any point if they feel that their privacy rights are being infringed. According to Aida (2020), Singapore’s Trace Together Covid-19 tracing app stands better chances of being effective if the people become educated on its importance. The reason is that the system provides voluntary participation but lacks in convincing the people.

1. **Transparency of the collected data**

Transparency in the amount and type of the data collected by Covid-19 contact tracing smartphone applications is crucial for monitoring and evaluation. All contracted entities and the government need to publicly account for the information they collect to allow for transparency. According to (Guinchard, 2020), very few users know what exactly the contact tracing program is doing on their phone. However, some users do not understand that the program continuously runs uninterrupted in the background for as long as the tracking entities want. The lack of information on the operation of these programs by the public is an avenue for exploiting their privacy rights.

The most vulnerable group, in this case, is the elderly who have access to smart devices. It is because they might be duped by unsuspecting parties to opt-in for the surveillance without necessarily understanding the tracing parameters. Therefore, it remains imperative for the program's working and the nature of the data to be explained in public domains. Similarly, the contents of RPIDs need to be explained and how that information could potentially harm the user. There are currently efforts by Google and Apple to provide public databases where the collected data will be available to allow the public to understand what is collected and how it is used (Loi, 2020). This move is driven by transparency; however, it is limited by governmental interferences through the power of withholding information and the national intelligence's need for secrecy.

1. **Security of the RPIDs**

The rolling proximity identifiers, as earlier shown, consist of information logs exchanged between two devices that have been in close contact for duration significant enough to warrant the transmission of the Covid-19 virus from one user to the other (Yasaka, Lehrich & Sahyouni, 2020). The frequency of the transmission of the Rolling Proximity Identifiers (RFIDs) has been tied to the security with concerns that transmitting them once every 24hrs can allow hackers to gain access to a log file containing all the information of the day’s activities of the user. Therefore, the frequency of transmission needs to be reduced as much as possible. Shortening the time required by the contact tracing program will make it safer and limit the amount of leaked data in the Rolling Proximity Identifiers (RPID) being intercepted by malicious parties.

Another solution for Rolling Proximity Identifiers (RPID) security would be the encryption of the whole process. The assignment of unique encryption codes to the Rolling Proximity Identifiers (RPID) would secure it from being used by unauthorized parties (Ahmed et al., 2020). Similarly, the assignment of unique codes to the Rolling Proximity Identifiers (RPID) in analysis databases would limit hackers' ability to backtrack Rolling Proximity Identifiers (RFID) to the identity of the user. It means that the user's personal information should not be stored in the same database as contact tracking information. Their information should only be looked up when they have been within proximity of an infected person. Lastly, the contact tracing entities need to protect false Bluetooth beacons broadcasting mimicked information used by hackers. The identifier keys of users need to be rotated frequently to avoid easy pinpointing of a particular phone as the source of a string of RPIDs, which would expose the user to cybercrimes (Li & Guo, 2020).

1. **Minimization**

Minimizing the amount and nature of the information collected by the contact tracing app will allow for the minimization of the risks to users. Different contact tracing application programming interfaces (APIs) are programmed to collect varying information ranging from phone numbers, email addresses, and in some cases, beacons of some locations. According to Li and Guo (2020), Singapore’s Trace Together requires the users to share their contact information while Google and Apple APIs only require unique identifier keys that can be pinged on public databases to contact the individual. This means that the Trace Together API is collecting unnecessary data that can potentially harm the user in hacking. Therefore, minimal and only Covid-19 related information should be collected to avoid data mining of private information.

**5.0 Conclusion**

The Covid-19 situation in the world is difficult to predict when it will end, and therefore we have to evolve to stay safe until viable vaccines are availed. However, before a viable Covid-19 vaccine is developed, every citizen must adhere to all the anti-COVID-19 measures prescribed by the World Health Organization. Notably, contacts tracing apps and other surveillance measures have been put in place to better monitor positive parties' interaction with negative parties. However, these measures' installation and execution have come with unnecessary exposures and violation of an individual's privacy rights.

In worst cases, the contact tracing apps have opened up our information to hackers who can falsely misrepresent themselves as nearby contacts. However, they are beacons ready to siphon data as well as install malicious payloads. However, their use has significantly aided in mitigating Covid-19 fatalities with infections being treated well in advance before the patients succumb. Therefore, Covid-19 tracing apps can be considered an ethical dilemma because it is useful on the one hand and is intrusive on the other. This dilemma raises the question if we should jeopardize our rights to privacy in the race to end Covid-19. Is it a worthy tradeoff?

**6.0 Future Directions**

The future of contact tracing apps is currently unknown due to the many possibilities that can arise from it. Governments and intelligence agencies have been continuously investing in ways within which it can conduct surveillance on people. Data is addictive in the sense that it becomes hard to stop once you start to collect it. It means that these entities could use the current Covid-19 tracing apps as the pilot stage for people's mass surveillance through their mobile phones. Therefore, the future could be riddled with data mining packets installed in our phones by governments and other entities.

Therefore, in anticipation of this, it becomes imperative for developers and information technology experts to start the development of countermeasures. It is also essential to ensure the protection of human rights to privacy by the assurance that the Covid-19 contact tracing apps will expire with the ending of Covid-19. Artificial intelligence should also be integrated into the contact tracing system to identify false Bluetooth beacons quickly. Furthermore, the AI system can be more useful in protecting user phones against manipulation by parties with malicious intent.

**References**

Ahmed, N., Michelin, R., Xue, W., Ruj, S., Malaney, R., Kanhere, S., Seneviratne, A., Hu, W., Janicke, H., & Jha, S. (2020). A survey of COVID-19 contact tracing apps. *Sage Journal*, *8*.

Bengio, Y., Ippolito, D., Janda, R., Jarvie, M., Prud'homme, B., Rousseau, J., Sharma, A., & Yu, Y. W. (2020). Inherent privacy limitations of decentralized contact tracing apps. *Journal of the American Medical Informatics Association*.

Dropkin, G. (2020). COVID-19: Contact tracing requires ending the hostile environment. *British Medical Journal*.

Fahey, R., & Hino, A. (2020). COVID-19, digital privacy, and the social limits on data-focused public health responses. *International Journal of Information Management*.

Frith, J., & Saker, M. (2020). It is all about location: Smartphones and tracking the spread of COVID-19. *Sage Journals*, *6*(3).

Gorji, H., Arnoldini, M., Jenny, D., Hardt, W., & Jenny, P. (2020). STeCC: Smart testing with contact counting enhances COVID-19 mitigation by Bluetooth app-based contact tracing.

Guinchard, A. (2020). Our digital footprint under COVID-19: Should we fear the UK digital contact tracing app? *International Review of Law, Computers & Technology*.

Iacobucci, G. (2020). COVID-19: Is local contact tracing the answer? *British Medical Journal*.

Janda, Y., Bengio, R., Yu, Y., Ippolito, D., Jarvie, M., Pilat, D., Struck, B., Krastev, S., & Sharma, A. (2020). The need for privacy with public digital contact tracing during the COVID-19 pandemic.

LI, J., & Guo, X. (2020). Global deployment mappings and challenges of contact-tracing apps for COVID-19. *SSRN Electronic Journal*.

Loi, M. (2020). How to fairly incentivize digital contact tracing. *Journal of Medical Ethics*.

Martinez, N., Wieten, S., Magnus, D., & Cho, M. K. (2020). Digital contact tracing, privacy, and public health. *Hastings Center Report*, *50*(3).

Oswald, M., & Grace, J. (2020). The COVID-19 contact tracing app in England and ‘Experimental proportionality’. *SSRN Electronic Journal*.

Ponce, A. (2020). COVID-19 contact-tracing apps: How to prevent privacy from becoming the next victim. *SSRN Electronic Journal*.

Rowe, F. (2020). Contact tracing apps and values dilemmas: A privacy paradox in a Neo-liberal world. *International Journal of Information Management*.

Ryan, M. (2020). In defence of digital contact-tracing: Human rights, South Korea, and COVID-19. *International Journal of Pervasive Computing and Communications*, *16*(4).

Van, H., & Ruijter, A. (2020). COVID-19 and privacy in the European Union: A legal perspective on contact tracing. *Contemporary Security Policy*, *41*(3).

Veloso, A., & Ziviani, N. (2020). Explainable death toll motion modelling: COVID-19 narratives and counterfactuals.

WHO (2020). WHO Coronavirus Disease (COVID-19) Dashboard. <https://covid19.who.int/>

Wilson, A., Warrier, A., & Rathish, B. (2020). Contact tracing: A lesson from the Nipah virus in the time of COVID-19. *Tropical Doctor*, *50*(3).

Yasaka, T., Lehrich, B., & Sahyouni, R. (2020). Peer-to-peer contact tracing: Development of a privacy-preserving smartphone app. *JMIR mHealth and uHealth*, *8*(4).

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)*.