Privacy and Contact Tracing in the Era of COVID-19

Raaghavv Devgon and Megan Skrobacz
MSCS Program, Northeastern University

***Abstract*—Currently we are in the middle of a serious pandemic. As there is no known, proven cure or vaccine which can help reduce the impact of COVID-19, multiple countries are choosing to endorse the method of contact tracing to try and contain the spread. Contact tracing can be implemented manually, but for this paper we will be evaluating tech solutions utilized by the governments of multiple countries in various forms. e will analyze contact tracing strategies used by Singapore, Australia, South Korea and Switzerland, as well as the Google/Apple API that allows for several contact tracing apps to function. We will evaluate the security and privacy concerns associated with these solutions, how different they are from each other in their implementation, and the vulnerabilities associated with them. Finally, we will holistically discuss the subject of contact tracing, seeking to understand whether there could be an ideal implementation of contact tracing in the future, given the inherent problems it must overcome to be effective.**

I. Introduction

Contact tracing[1] is the process of identifying a person who may have come into contact with an infected individual, and the subsequent collection of further information about these contacts. Due to the infectious nature of COVID-19, there has been a significant rise in contact tracing. Many governments have allotted effort for manual contact tracing, which involves human interaction with infected patients to systematically identify individuals with whom a patient was in contact with and perhaps infected. While this is a sound mechanism, some countries have looked instead to tech solutions. A common method we shall discuss involves utilizing citizens' smartphones via apps which effectively turn the platform into a 'tracking device' as a means to hasten the tracing and make it more efficient. For this purpose, apps developed can use location-based services (GPS), which allow authorities or health officials to track the movements of a phone's owner. Other methods have also been implemented, such as using Bluetooth to track how many devices encountered the other within a specified range and time frame. Each of these means have associated pros and cons. Due to the nature of these apps, there is also hesitation amongst citizens – "*How much information are they storing about me?"* or *"How much are they tracking my movements?"* are often common concerns. In short, the concern is: "*How do these apps affect or infringe one's privacy, and is it worth the cost?"* It's a prudent question, especially in today's time, where a person's personally identifiable information (PIIs) such as health information can be exploited and monetized. There are several laws across the world which help enforce the protection of such information such as Fair Information Practices Principles[2], GDPR[3] and HIPPA[4]. Due to the nature of the pandemic, these laws in some cases have been relaxed in some regions so health institutes can leverage the information for research and public health purposes.

Some countries have introduced specific COVID-19 apps and tech solutions using contact tracing. In this paper we will be analyzing the apps developed by Singapore, Australia, South Korea and Switzerland. We will be providing a detailed analysis on each of these apps, with particular regard to: the system design; how and where the data is stored; what kind of information is stored; the vulnerabilities and privacy issues associated with these apps; and how successful they actually are. We will also be evaluating Google and Apple's APIs which, at the time of this paper, were only just released.

The paper is divided in the following format:

Section II will go into further detail about the difference between centralized and decentralized approaches to contact tracing. Section III addresses the empirical analysis of the contact tracing strategies that were deployed in Singapore, Australia, and South Korea. Section IV looks at new or upcoming technologies in development which might offer a different option in the current climate, namely Switzerland's upcoming app as well as Google and Apple's API. In Section V, we will take a step back from specific contact tracing implementations and instead look at contact tracing holistically, discussing problems inherent with the process in general. Finally, in Section VI, we discuss alternate ideas to the traditional implementations of contact tracing using GPS or Bluetooth, while Section VII will offer the conclusion of our research.

II. Centralization vs Decentralization

Before we discuss specific implementations of contact tracing, it's helpful to understand the difference between centralized and decentralized approaches to contact tracing.

A centralized approach takes the pseudonymized proximity data from contact tracing implementations and stores and processes it on a central server for future use. Typically, these servers are controlled by a national authority, such as a healthcare service. With this approach, while providing the efficiency benefit of having a single database for querying, prompts concerns of increased risk of function creep and state surveillance, as well as potential for hacking.

By contrast, a contact tracing infrastructure that is decentralized[5] heavily depends on the concept of ephemeral IDs. In this implementation, IDs which represent the user, as well as IDs the user has encountered, are stored locally on a device. When a user provides consent after a confirmed

COVID-19 diagnosis, that user's ID would be broadcasted via a relay server to all users, thereby enabling devices to locally compute when the user was in contact with that ID. In this manner, there is no need for a centralized database to keep track of interactions and infected patients.

The centralized approach has been backed by France and the UK part of the PEPP-PT[6], a homegrown standardization effort. Germany[7], like the UK and France, was originally part of the PEPP-PT initiative, but since then have also been supportive about decentralized infrastructure. As of the time of this paper, there were concerns regarding lack of transparency around the PEEP-PT model and the protocols it would support. This was bolstered by the fact that no code has yet been published for analysis and review.

III. Contact Tracing Apps In Use

In this section we will discuss the contact tracing apps which have been deployed in Singapore, Australia and South Korea. For each approach, we will cover how they work, what privacy-preserving measures they employ, and evaluate their approach in the hopes of providing a thorough and standardized overview of each implementation.

A. Singapore

Singapore's TraceTogether[8] app was launched on March 20, 2020. It was one of the first countries in the world to offer a contact tracing solution and many suggest it also created a blueprint[9] for the development of contact tracing apps. The app installation is voluntary in nature, and users must provide their mobile number and identification details during download. Once downloaded, a randomized user ID is generated, which helps to map the rest of the user information within its storage on a private centralized server. While it's mentioned that the app doesn't use GPS and data related to WiFi or mobile network information, the app does collect additional personal information such as device information (brand, category, model , OS, version) and statistics regarding app usage (the store it was sourced from, the version, a user's country, a user's language, time since installation and usage statistics).

How it Works: When a person is close to another phone running the app, both phones will use Bluetooth to exchange a temporary ID via a token. The temporary ID is generated by encrypting the user ID with a private key held by the Ministry of Health. Every 15 minutes, a device will change its token to help protect the identity of the user. Data collected is stored securely on the phone and is only shared with the Ministry of Health when one tests positive for COVID-19. Health officials act as a central governance body; once a person tests positive, the information about how many people might have encountered that individual is sent to a manual contact tracer to analysis and possible interference.

Privacy-Preserving Measures:

- The anonymized Bluetooth data stored on the phone is automatically deleted after 25 days
- It is possible to disable the functionality of the app at any time by turning the app's Bluetooth permissions off or deleting the app
- Installation is voluntary
- Data is collected and stored on the device

Evaluation of this Approach: TraceTogether overall hasn't been able to match the expectations it set to achieve. The app currently has been downloaded by only 1.4 million people, which means around 5.6 million people have not utilized this technology. The National Development Minister of Singapore, Mr. Lawrence Wong, stated that the app needs to be downloaded by three quarters of the population for it to be truly effective. This has sparked speculation as to whether the app should be made mandatory for download.

According to a survey conducted by Singapore-based independent pollster Blackbox Research, 45% of respondents did not download the TraceTogether. The main consideration was that the participants of the survey didn't want the government tracking their movements, even though Singapore is the 11th most-surveilled city in the world[10].

Public distrust in contact tracing could also be compounded due to past instances of cyberattacks on government databases. In June 2019, hackers copied the hospital records of more than 1.5 million patients, of which 160,000 had information about their outpatient-dispensed medicines exposed. The incident was described by the authorities as a "serious breach of personal data"[11]. Additionally, there might also be concern from the public as the Personal Data Act[12] in Singapore doesn't apply to the government.

Other than privacy concerns, some users were also dissatisfied with the app's interface, which was far from user-friendly. The app was also said to be less than effective as smart phones would turn off the Bluetooth when the app wasn't in use to save power.

To tackle the ineffectiveness of the app, Singapore is planning to hand out a simple wearable device to each of its citizens to track those who have been exposed to the Coronavirus[13].

B. Australia

Australia announced its own contact tracing app, called COVIDSafe[14], on April 26, 2020. This implementation is somewhat akin to Singapore's TraceTogether, as it utilizes Bluetooth as the main mechanism for capturing traces. However, COVIDSafe requires more information from users during download than TraceTogether, namely a user's mobile number, name/pseudo-name, age range and zip code.

How it Works: When the app detects that a user has been in contact with another user, it records the contact's encrypted user ID (which changes every 2 hours), the date and time of contact, and the Bluetooth signal strength. This data is then stored in the National COVID-19 datastore. The key difference between TraceTogether and CovidSafe is that in the case of a potential infection, a health official will contact a person who has been in contact with COVID-19 patient directly rather than being approached by a manual tracer (who may or may not have any medical training) as with TraceTogether.

Privacy-Preserving Measures:

- Installation is voluntary
- COVIDSafe governed by the Privacy act of 1988[15] and the Biosecurity Determination of 2020[16]
- The app doesn't track GPS movements
- The user can download a copy of whatever data the app has on them
- The data is stored on the device and is deleted after 21 days
- The app requires patient consent before accessing any data on a device
- The app implements two-factor authentication to gain user consent
- There is also an option to delete PIIs of a user
- The source code of the application has been made public

Evaluation of this Approach: For the app to function effectively, it was determined that 40% of the Australian population had to install and use it. Currently, the number of active users is 1.5 million below that target. Critics have also noted that there is a problem expressing a target as a percentage of the population, as not every Australian has a smartphone and thus couldn't use such an app even if they wanted to do so[17].

To date, amusingly, only one infected person was ever detected as a result of COVIDSafe, raising serious concerns about its effectiveness. There is also no publicly-available white paper or server code for the app, which has raised issues with transparency[18].

C. South Korea

South Korea was one of the first countries to deploy a contact tracing strategy for COVID-19 containment; their solution was deployed in February, a time when other countries were still coming to grips with the far-reaching impact of the virus. However, unlike some other countries, South Korea's implementation extends beyond a contact tracing app. The country's technology can be summarized into three main components: a surveillance network which taps into city infrastructure to monitor citizens as they go about their daily lives; a contact tracing app to monitor visitors during the required two-week quarantine; and a contact tracing app called Corona 100m which broadcasts information from the government in regards to cases of infected individuals a user might have been in contact with. Put together, we would propose that this is the most aggressive strategy being currently utilized for COVID-19 containment, and perhaps the most concerning from a privacy standpoint.

In order to understand why South Korea chose such a comprehensive implementation, and how it did so in such a rapid manner, it's important to recognize the context of South Korea's history. As noted in Thompson's article from *The Atlantic*, in 2015, South Korea was hit hard by the Middle East Respiratory Syndrome (MERS) outbreak; the disease spread like wildfire through cities and hospitals, killing and infecting thousands. Many Koreans felt the government was inadequately prepared to handle another outbreak of such scale, and as such South Korea rewrote much of its infectious disease prevention legislation to prevent such a tragedy happening in the future. This legislation included allowing laboratories to use unapproved diagnostic kits during a public-health emergency, giving health authorities warrantless access to CCTV footage and geolocation data from patients' phones, as well as new laws which required local governments to send prompt alerts, such as emergency texts, to disclose the recent whereabouts of new patients[19]. As such, when Coronavirus became a worldwide pandemic, the country was well-prepared to quickly adopt strict containment measures.

How it Works: The crux of South Korea's strategy of containment depends on what it calls "Smart Cities", a concept which was initially designed to share information between cities on things like traffic and pollution, but is now being used to reduce time to find and isolate Coronavirus cases. It consists of a database, managed by the federal government, in which agents from the Korean Center for Disease Control can access CCTV footage, credit card transaction data, travel information, and location data to keep tabs on citizens as they go about their daily lives. Along with information uploaded by the KCDC, the system compiles data from the National Police Agency, the Credit Finance Association of Korea, three telecommunications companies and 22 credit card companies[20]. This system does not require the consent of those being surveilled.

Once a person has been confirmed to have Coronavirus, the KCDC taps into this system to figure out the route the patient took, whether their house has been disinfected, whether they were in contact with anyone, and whether they were wearing a mask the entire time, and broadcasts this information to its citizens via its website. On the website, each patient is identified by their gender and their age[19]. Additionally, the government will also text citizens who live within a specified radius of the infected individual.

For citizens who have downloaded the Corona 100m app, their movements are tracked daily via GPS data from their device and compared to the routes broadcasted from the government. If it has been determined that the user was within 100m of an infected individual, the app alerts the user to get tested. The app will also map locations with higher concentrations of known cases to direct individuals to avoid these areas[22].

For all visitors to South Korea, the government mandates that all people must be screened at the airport for COVID-19, as well as download a contact tracing app. To do so, they must input information such as their passport info, nationality, name, and address where they will be staying. They must then self-quarantine for two weeks. Using location-based contact tracing, the app ensures that the user does not break quarantine by informing health officials if the user has left the premises where they should be staying. Additionally, the app requires users to input their health vitals daily, so that health officials can determine whether there is a chance that a user might be showing symptoms of COVID-19, in which case a user can use the app's interface to get in contact with local health authorities. Finally, after

the mandated two-week quarantine is over, the app informs users when they are free to delete it from their phone[21].

Privacy-Preserving Measures:

- The Corona 100m is voluntary in nature
- When an infected individual is identified, their name is removed
- Police approval is needed if investigators want information from the database to track an individual
- Only a small number of people have access to the database itself

Evaluation of this Approach: South Korea's approach does come with a whole host of privacy concerns - in particular, the idea of surveillance without consent, both in the smart cities tracking as well as the mandatory contact tracing app for visitors, can be viewed as extremely problematic to privacy in many cultures around the world. Additionally, as the data is centrally-held by the government, it could be seen as a concern that people's private data might be used for other purposes once the pandemic is over and has a potential to be hacked. Finally, the sheer amount of information that South Korea releases about COVID-19 patients makes it far easier, in contrast to other implementations, to identify a patient with a little bit of intuition or linkage attacks.

Regardless of these privacy concerns, South Korea's approach seems to have been effective at curbing the outbreak; despite having the second-highest number of COVID-19 cases in the word at the end of February, with almost a thousand new cases a day, by mid-March they reduced that number down to less than a hundred new cases per day. As of the time of this paper, that infection rate has remained constant with no new spikes in infections[23].

Part of South Korea's success probably lies in its approach to surveillance via Smart Cities. According to the Ministry of Land, Infrastructure and Transport, combining artificial intelligence with the databank cuts down the time needed to trace a patient's movements from one day to only ten minutes[20].

As for public opinion of these measures, the Corona 100m app has been reportedly downloaded more than a million times, with overwhelmingly positive reviews[24]. While it seems as though the populace is tolerant of current approaches for now, time will tell if public opinion shifts once a vaccine and cure is in place.

IV. Contact Tracing Approaches in Development

A. Google/Apple API

On April 10, 2020, Google and Apple united in a joint effort to develop APIs[25] for their phone operating systems which would help governments develop their own apps based around a decentralized framework. At the time of this paper, these APIs have only recently been pushed, and no app has yet been fully implemented using this framework.

How it Works: Applications built on this framework will harness Bluetooth signals to track traces. To do so, a user must first enable the technology. Once enabled, an app utilizing this API will regularly send out a beacon via Bluetooth. The beacon possesses a random Bluetooth identifier, which is anonymized and isn't tied to the user's identity. The identifier is also ephemeral, as it will be changed every 10-20 minutes.

When another user's smartphone is within a defined proximity to another device, the two devices will share and record each other's beacons and subsequent identifiers. The system also keeps track of when the interaction happened, how long it lasted, and the Bluetooth signal strength of the contact. At least once per day, the app will download a list of the identifiers from confirmed COVID-19 patients. These identifiers are then validated against the identifiers logged by the phone. If a match is found between the two, the user is notified.

Privacy-Preserving Measures:

- User information will never be shared with Apple or Google
- A user will have the option to turn on or off the technology by design
- If a user decides to participate, the data will only then be shared with the health officials only when either a user has tested positive or has encountered someone who tested positive
- The mechanism for allowing users to report themselves as positive will be determined by the relevant public health authorities
- Only public health authorities will have access to this technology and their apps must meet the specific criteria regarding privacy, security and data control
- Public health authorities will also be required to set a minimum threshold for time spent together, such that a user needs to be within a Bluetooth range for at least five minutes to register a match. If the contact is longer than five minutes, the system will report time in increments of five minutes up to a maximum of 30 minutes to ensure privacy.
- Another alternative these two companies have planned is to send out and listen to the Bluetooth beacons, but without an app. This feature is available in iOS 13.5, which includes a new COVID exposure notification feature.

Evaluation of this Approach: The API developed by Apple and Google hasn't been used by many countries at the time of the writing of this paper. While there have been talks to implement the API in the United States, there are still concerns amongst privacy experts regarding its implementation.

B. Switzerland

Switzerland is one such country which is working to develop a decentralized contact tracing app, called 'DP-3T'

or SwissCovid[26], which will use the API framework provided by Apple and Google. This app is being developed by two Swiss federal institutes of technology in Zurich (ETH Zurich) and Lausanne (EPFL). The researchers from these institutes were also the part of the European Privacy-Preserving Proximity Tracing or PEPP-PT project which was discussed previously. However, due to their privacy concerns regarding the use of a centralized framework, they withdrew from the group and started to work on their own decentralized system. The system has gained support by other countries in Europe, namely Italy and France.

How it Works: Although it has not been fully implemented, a pilot phase was launched on May 13, 2020 for a certain group of the population until the end of that month as per the order of the government. The DP-3T system is decentralized, with contacts and data stored on devices rather than on an external server. The application is unique due to the way it's being carefully introduced to the public and the privacy-preserving stance the government has on it.

Privacy-Preserving Measures: The Swiss House of Representatives and Senate approved a proposal which urged the government to prepare a bill to ensure the app is specifically defined under Swiss laws. This measure ensures that the app will be subject to the safeguards set out in Swiss privacy law.

Authorities have also released the source code[27] of the SwissCovid app to the public to allow experts and security professionals to detect any risks related to security and privacy with the app before it is officially launched to the public. The National Cybersecurity Centre (NCSC) will also receive the test reports sent by the public via an online form[27], which allows those testing the app in the pilot phase to report any issues before being released to the public. It will then review the submissions, set their priority based on the severity of the problems detected and make the necessary adjustments. The results will be updated daily and made available on the NCSC website[28].

As of June 12, 2020, ten security related bugs have been found, out of which seven have been fixed. Once testing is completed in the pilot phase, Swiss parliament will evaluate if the app can be launched publicly based on their findings as to whether the app upholds privacy standards[29].

Evaluation of this Approach: The app hasn't been made available to the public at the time of the writing of this paper, so presently we are unable to fully evaluate this app. Time will tell if this method is truly more privacy-preserving than previous implementations.

V. Contact Tracing – A Holistic View

A. Major Themes with Contact Tracing

Despite the different implementations we've covered in this paper, and the inherent pros and cons of each framework, two major themes have emerged across all implementations.

First and foremost, there does not seem to be one single, uniform "best practice" when it comes to contact tracing. In fact, there have been resources allocated to simply keeping track of the different contact tracing apps being utilized around the world for COVID-19, such as within MIT's *Technology Review*[30]. This has serious implications on the impact this technology can have on containing the spread of COVID-19 across the globe. Undoubtedly, certain implementations will be more effective at stopping the spread of the virus, while others will fall decidedly short of doing so. Without a unified world effort to commit to this technology evenly, humans as a species are effectively combating a global threat with an uneven playing field. Additionally, for the millions of people who travel internationally, this translates to the reality of potentially having to download a different app for each country they visit, thus compromising their privacy.

The second theme we identified, and perhaps most crucially, is that the success of a contact tracing strategy seems to be centered around one simple thing: getting enough people to adopt the technology. Some countries like South Korea had no problem with this execution due to mandates like mandatory downloading of contact tracing apps, providing temporary smartphones to those without for said apps, and government surveillance. However, for countries where use of these apps is voluntary, this technology will only work if a huge percentage of the population agree to use it. In fact, according to many experts, at least half of a population need to download and use the app for it to be effective [36].

As noted in the study from Kaptchuk et al[31], there are numerous factors that play a part in a person's decision to download such an app. First and foremost, the population must trust the agency that is running the app. For example, Katuchuk et al's study showed that Americans are more willing to install a contact tracing app provided by a public health agency or a health insurance provider than one distributed by the federal government[32]. Similarly, the perceived efficacy of the app matters, specifically in regards to privacy. In a 2018 study conducted by the SAS Institute, 73% of Americans felt that their concern over the privacy of their personal data has increased in the past few years[33]. Combined with the results from Kaptchuk et al's study, which showed a decreased willingness to adopt a contact tracing app with low privacy-protecting measures, we can conclude that, at least in the US, apps which do not make privacy a priority will have poor adoption rates, and thus less overall impact.

User environment has proven to be another huge factor which can affect app adoption. For example, in some US states, such as South Dakota, local governments also offer COVID-19 apps[34], so any national implementation could see consumers having to choose one app over another, thus decreasing individual app adoption rates. Furthermore, for millions of people in the word, access to smart devices is beyond their reach, so any contact tracing solution by design excludes them. This is doubly unfortunate considering that often those without access to this technology are perhaps the ones that would most benefit from it, as groups such as the poor, minorities, or homeless are hardest-hit by the COVID-19 virus[35] [37].

B. Common Vulnerabilities with Contact Tracing

In addition to common themes with contact tracing implementations, there are also several shared vulnerabilities with this technology. In our attempt to analyze contact tracing holistically, we shall identify a few of the most prevalent matters.

First, and perhaps most concerning, is the overall threat of reidentification - that is, the ability to ascertain the identity of an individual who may have COVID-19 despite PIIs being removed from a dataset. For example, in South Korea, it is possible a to make an educated guess as to who has COVID-19 by looking at the age, sex, neighborhood, and path of the individual who reported positive. This is what Chan et al classify as an inference attack[38]. Additionally, reidentification can happen with a physical attack, in which an attacker gains access to a user's phone, thus enabling them to see, by opening the app, whether that user has tested positive for COVID-19.

Both these possibilities also highlight another shared vulnerability of this technology - a threat of compromising privacy. In addition to reidentification attacks, privacy can be compromised if the data is centralized and held by a potentially untrustworthy party, or one that might use said data for other purposes. For example, as noted in Katuchuk et al[31], Americans tend to not trust big tech companies with their data, displaying a lack of faith that their privacy will be protected or that their data won't be used for other purposes beyond protecting against COVID-19, such as making a profit [31]. To their credit, some implementations of contact tracing do include promises that centrally-held data will be deleted periodically or at least once the pandemic is over, however time will tell how enforcing this promise can be carried out. Additionally, these methods don't necessarily protect against other vulnerabilities to privacy, such as the ability for this technology to be used for overall or unwarranted surveillance of a population. An obvious case here is South Korea, where contact tracing does not require consent from any civilian living within smart cities.

Finally, contact tracing as a practice has several vulnerabilities related to reliability, here defined as an app's ability to accurately alert users who may have been in contact with a positive COVID-19 patient so they can get tested or self-quarantine. Reliability can be compromised in many ways; for instance, Chan et al mention the threat of replay attacks[38], in which multiple attackers impersonate a single user, put themselves in contact with as many people as they can, and then one reports themselves as COVID-positive, thus creating a false-positive alert for any person who was in contact with any one of the attackers. This ability to self-report in itself can be an issue to reliability even without a replay attack, as a single malicious user could, for example, report themselves COVID-positive while in a location with a large number of passersby, therefore potentially affecting the ability of that location to function effectively if those within it are encouraged to leave and self-quarantine, or if others are hesitant to enter the area for fear of catching the virus. For example, in South Korea's Corona 100m app, a "heat map" feature identifies areas that have had high numbers of COVID-19 patients; this could be detrimental to businesses if attackers spammed false positives while in a specific location, increasing the risk factor of visiting that venue in the eyes of potential customers. Additionally, as we saw with Singapore's TraceTogether app, poor UI could lead to unreliable data and weak performance, as users who are COVID-positive may struggle to understand the interface for reporting themselves positive, thus leading to false negatives.

VI. Looking Towards the Future

In addition to the types of implementations we've covered, there are also some technologies that can perhaps be considered as alternatives to the implementations of contact tracing currently in practice, or even used in addition to contact tracing to improve efficacy. While the details of specific implementations are beyond the scope of this paper, as a thought experiment, here we will highlight a few that can potentially be used to assist with slowing the spread of COVID-19 while preserving privacy.

A. Blockchain

As we've seen, contact tracing for COVID-19 has typically utilized GPS or Bluetooth technology as the backbone for tracking traces – in particular, Apple's and Google's API heavily depends on Bluetooth. However, as this framework is present on the phone's OS with the recent software update, some privacy advocates worry that companies might already be collecting data. It is especially concerning as the technology will be present on one's device, without downloading the app which requires this feature. Therefore, perhaps there is a better solution which could potentially address the privacy and transparency issues.

Although we leave the specific details of implementation to experts, we propose blockchain could potentially be the answer in this situation[39]. Blockchain's strongest benefit is arguably its transparency and immutability. When data is introduced into the blockchain platform, it is organized in blocks. Attached to each block of information is a hash value for that block and for the previous one, ensuring retroactive "linkage" between them. This is how data becomes stable and cannot be changed, deleted or tampered with.

Using a blockchain-based app, users can opt for data to be shared from the devices they specify. This process creates a digital identity which can join a digital distributed ledger (blockchain) that records who has downloaded the data sharing app. Each device would submit its unique Bluetooth identifier and the other participants on this ledger would be able to validate that a device has opted to share and receive anonymous information. This forms the basis of consent to be a participant in this data sharing and subsequent 'tracking' via the app.

The ledger, or blockchain, has the additional benefit of registering the time and date (a timestamp) of participation and a user has complete visibility of which devices have opted into the network. Blockchain is immutable and cryptographically secure, creating a record that acts as 'a single source of truth of who opted in, searchable in a matter of seconds.

Finally, this blockchain ledger will enable health authorities to keep a medical record of the owner of one specific device and facilitate the tracking of medical information associated with an anonymous device identifier. This way, everyone participating on the system could see if they have been near another person that owns a device that has been recorded on the network as infected (without that person being identified).

B. Ultrasound

Many app implementations of contact tracing for COVID-19 utilize Bluetooth Low Energy (BLE) to improve performance; however, so too do many other apps and devices. As such, this can cause some interference or lead to some other apps to use the BLE to broadcast their own information unknowingly. Additionally, it's been noted that BLE can also be susceptible to DDOS attacks[40], where a modified attack akin to buffer overflow can impact the storage of mobile devices.

Therefore, another proposed alternative to this approach would be to use ultrasound waves along with Bluetooth technology. In this approach, Bluetooth would allow a device to sense nearby devices, and the microphone would detect inaudible sounds passed between a phone to other devices. It could then use these ultrasounds to determine a user's proximity to others without using their location or having access to the personal information of that device.

This approach has been developed by the researchers and collaborators at Carnegie Mellon University. They have developed an app which they call NOVID[41]. However, there is an issue with this approach as the microphone is required to always be turned on for the app to function, which does raise concerns about one's privacy.

VII. Conclusion

Despite the great intentions of this technology, our research has led us to conclude that contact tracing is certainly not the "silver bullet" that it is sometimes touted to be in regards to stopping the spread of Coronavirus. By all accounts, contact tracing is here to stay, at least for the duration of this pandemic. However, if this technology is to be used, we should be concentrating on the data derived from contact tracing and making efforts to ensure that it does not further inequality in the societies where it is implemented. This will yield greater dividends for privacy – and by extent adaption rates and efficacy - rather than focusing on the technology itself.

As noted previously, for this technology to produce results, typically at least half of the population needs to use it. Let's say, for sake of argument, that in the United States everyone who was able to download such an app did so and used it flawlessly. In theory, wouldn't this mean that our data would be reliable, and policies using this information to track contagion rates would be maximally effective?

The reality, though, is that this data - even in this perfect scenario - will always be inherently flawed, because it excludes a subgroup of people that are often most hard-hit by COVID-19: those without access to smartphones. Thus, enacting policies based on contact tracing data is almost akin to a "pay to win" situation; those who are affluent enough to afford smartphones benefit from policies which become less strict when their subgroup is safe, while those who can't participate can only sit on the sidelines and hope that these policies erode protections that otherwise would stop the virus from ravaging their communities. This, by definition, is textbook inequality.

We also believe that serious consideration should go into who specifically has access to COVID-19 data generated from public contact tracing implementations, as there is tremendous opportunity for financial exploitation for parties looking to make a profit. For example, some life insurance companies are already raising rates for policyholders who admit having traveled in "high risk" areas [42]. Imagine how many more thousands, or even millions, of people that could negatively be impacted by such tactics if this information was freely available to profit-driven companies. Otherwise actionable information could simply lead to personal harm.

Thus, efforts to increase PETs for publicly available data - or mechanisms to perhaps limit what specific data certain parties could see - could be arguably just as important as the method of obtaining that data itself through contact tracing. We therefore encourage others interested in furthering research into the topic of contact tracing to focus more on the implications of the data being collected rather than the implementation of contact tracing itself.

References

[1] "Contact Tracing". *Wikipedia.* Retrieved from https://en.wikipedia.org/wiki/Contact_tracing

[2] Gellman, Robert. "FAIR INFORMATION PRACTICES: A Basic History". October 2019. Retrieved from https://bobgellman.com/rg-docs/rg-FIPshistory.pdf

[3] "General Data Protection Regulation (GDPR)". *Intersoft Consulting.* Retrieved from https://gdpr-info.eu/

[4] *Health Insurance Portability and Accountability Act (HIPPA).* Retrieved from https://www.hhs.gov/hipaa/index.html

[5] Ronald L. Rivest, Daniel J. Weitzner, Louise C. Ivers, Israel Soibelman, Marc A. Zissman, "PACT: Private Automated Contact Tracing". May, 2020. Retrieved from https://pact.mit.edu/

[6] Lomas, Natasha. "Germany ditches centralized approach to app for COVID-19 contacts tracing". *TechCrunch*, April 2020. Retrieved from https://techcrunch.com/2020/04/27/germany-ditches-centralized-approach-to-app-for-covid-19-contacts-tracing/

[7] *Pan-European Privacy-Preserving Proximity Tracing*. Retrieved from https://www.pepp-pt.org

[8] *TraceTogether*. Retrieved from https://www.tracetogether.gov.sg

[9] Hyunghoon Cho, Daphne Ippolito, & Yun William Yu. "Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs". March 2020. Retrieved from https://arxiv.org/pdf/2003.11511.pdf

[10] Bischoff, Paul. "Surveillance camera statistics: which cities have the most CCTV cameras?".*Comparitech*, August 2019. Retrieved from https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

[11] "PDPA Overview". *Personal Data Collection Commission Singapore*. Retrieved from https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act

[12] Dewey Sim, Kimberly Lim. "Coronavirus: why aren't Singapore residents using the TraceTogether contact-tracing app?". *SCMP*, May 2020.Retrieved from https://www.scmp.com/week-asia/people/article/3084903/coronavirus-why-arent-singapore-residents-using-tracetogether

[13] Hale, Conor. "Singapore opts for countrywide wearables for COVID-19 tracing". *Fierce Biotech*, June2020. Retrieved from

https://www.fiercebiotech.com/medtech/singapore-opts-for-country-wide-wearables-for-covid-19-tracing-reuters
[14] "CovidSafe app". *Australian Government Department of Health*. Retrieved from https://www.health.gov.au/resources/apps-and-tools/covidsafe-app
[15] "Australian Privacy Act 1988." *Australian Government.* Retrieved from https://www.legislation.gov.au/Details/C2014C00076
[16] "Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020." *Australian Government.* Retrieved from https://www.legislation.gov.au/Details/F2020L00480
[17] Taylor, Josh. "How did the Covidsafe app go from being vital to almost irrelevant?". *The Guardian*, May 2020. Retrieved from https://www.theguardian.com/world/2020/may/24/how-did-the-covidsafe-app-go-from-being-vital-to-almost-irrelevant
[18] Stilgherrian. "Australia's wobbly start to COVIDSafe app transparency". *ZDNet*, May 2020. Retrieved from https://www.zdnet.com/article/australias-wobbly-start-to-covidsafe-app-transparency/
[19] Thompson, Derek. "What's Behind South Korea's COVID-19 Exceptionalism?". *The Atlantic*, May 2020. Retrieved from https://www.theatlantic.com/ideas/archive/2020/05/whats-south-koreas-secret/611215/
[20] Smith, Josh & Shin, Hyonhee & Cha, Sangmi. "Ahead of the curve: South Korea's evolving strategy to prevent a coronavirus resurgence." *Reuters*, April 2020. Retrieved from https://www.reuters.com/article/us-health-coronavirus-southkorea-respons/ahead-of-the-curve-south-koreas-evolving-strategy-to-prevent-a-coronavirus-resurgence-idUSKCN21X0MO
[21] The Government of the Republic of Korea. "Flattening the curve on COVID-19." *Ministry of the Interior and Safety*, April 2020. Retrieved from https://www.mois.go.kr/eng/bbs/type002/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000022&nttId=76748
[22] "Review of Mobile Application Technology to Enhance Contact Tracing Capacity for COVID-19." *Johns Hopkins Center for Health Security*, April 2020. Retrieved from https://www.centerforhealthsecurity.org/resources/COVID-19/COVID-19-fact-sheets/200408-contact-tracing-factsheet.pdf
[23] "COVID-19 pandemic data." *Wikipedia*. Retrieved from https://en.wikipedia.org/wiki/Template:COVID-19_pandemic_data
[24] Dujmovic, Jurica. "Wildly popular coronavirus-tracker app helps South Koreans steer clear of outbreak areas." *MarketWatch*, March 2020. Retrieved from https://www.marketwatch.com/story/wildly-popular-coronavirus-tracker-app-helps-south-koreans-steer-clear-of-outbreak-areas-2020-03-18
[25] "Exposure Notifications". *Google Inc and Apple Inc*, May 2020. Retrieved from https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.1.pdf
[26] DP3T - Decentralized Privacy-Preserving Proximity Tracing. Retrieved from https://github.com/DP-3T/documents
[27] *DP3T*. Retrieved from https://github.com/DP-3T
[28] "Reporting Form". *Reporting and Analysis Centre for Information Assurance MELANI*. Retrieved from https://www.melani.admin.ch/melani/en/home/public-security-test/reporting_form.html
[29] "Current Reports". *Reporting and Analysis Centre for Information Assurance MELANI*. Retrieved from https://www.melani.admin.ch/melani/en/home/public-security-test/current_findings.html
[30] Patrick Howell O'Neill, Tate Ryan-Mosley, and Bobbie Johnson. "A flood of coronavirus apps are tracking us. Now it's time to keep track of them." *MIT Technology Review*, May 2020. Retrieved from https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/
[31] Kaptchuk, Gabriel & Hargittai, Eszter & Redmiles, Elissa. (2020) "How good is good enough for COVID19 apps? The influence of benefits, accuracy, and privacy on willingness to adopt." Retrieved from https://arxiv.org/pdf/2005.04343.pdf
[32] Eszter Hargittai and Elissa Redmiles. "Will Americans Be Willing to Install COVID-19 Tracking Apps?" *Scientific American*, April 2020. Retrieved from https://blogs.scientificamerican.com/observations/will-americans-be-willing-to-install-covid-19-tracking-apps/
[33] "SAS Survey: 67 percent of US consumers think government should do more to protect data privacy." *SAS*, December 2018. Retrieved from https://www.sas.com/en_us/news/press-releases/2018/december/data-management-data-privacy-survey.html
[34] "Care19 | ND Response." *North Dakota State Government*. Retrieved from https://ndresponse.gov/covid-19-resources/care19
[35] Maxwell, Conner. "Coronavirus Compounds Inequality and Endangers Communities of Color." *Center for American Progress*, March 2020. Retrieved from https://www.americanprogress.org/issues/race/news/2020/03/27/482337/coronavirus-compounds-inequality-endangers-communities-color/
[36] Ng, Alfred. "Contact-tracing apps have a trust problem, even if they do protect your privacy." *C|Net*, April 2020. Retrieved from https://www.cnet.com/health/contact-tracing-apps-have-a-trust-problem-even-if-they-do-protect-your-privacy/
[37] Amos Toh and Deborah Brown. "How Digital Contact Tracing for COVID-19 Could Worsen Inequality." *Just Security*, June 2020. Retrieved from https://www.justsecurity.org/70451/how-digital-contact-tracing-for-covid-19-could-worsen-inequality/
[38] Chan, Justin & Gollakota, Shyam & Horvitz, Eric & Jaeger, Joseph & Kakade, Sham & Kohno, Tadayoshi & Langford, John & Larson, Jonathan & Singanamalla, Sudheesh & Sunshine, Jacob & Tessaro, Stefano. (2020). "PACT: Privacy Sensitive Protocols and Mechanisms for Mobile Contact Tracing." Retrieved from https://arxiv.org/pdf/2004.03544.pdf
[39] Angel Pateiro. "How blockchain can resolve the data privacy threats posed by contact tracing". *Financialit.net*, April 2020. Retrieved from https://financialit.net/blog/blockchain/how-blockchain-can-resolve-data-privacy-threats-posed-contact-tracing
[40] Peter Gullberg. "Denial of Service Attack on Bluetooth Low Energy". *ResearchGate*, September 2016. Retrieved from https://www.researchgate.net/publication/317063884_Denial_of_Service_Attack_on_Bluetooth_Low_Energy
[41] *NOVID*. Retrieved from https://www.novid.org
[42] Jennifer Bradley Franklin. "Can you get a life insurance policy during COVID-19?". *Bankrate*, June 2020. Retrieved from https://www.bankrate.com/insurance/life-insurance/coronavirus-and-life-insurance/