Page 1604 - 1612 **DOI:** *http://doi.one/10.1732/IJLMH.25883*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 1

2021

Contact Tracing Apps: Compromising Privacy in a Pandemic

RACHNA D DUBEY[1]

ABSTRACT

The COVID-19 global pandemic has brought the world to an impasse in 2020 and set off mandatory lockdowns all around the world to contain this lethal virus. With long quarantine periods and asymptomatic carriers, it had become challenging to track and restrict the virus. Technology played a vital role in combating the virus due to its accessibility and extensive reach. One such measure taken by countries to track the virus is the contact tracing apps like Aarogya Setu. However, these contact tracing apps raised many privacy concerns and posed a significant challenge to data protection and security. The right to privacy is elevated as a fundamental right, and any breach of this right is an attack on the constitution itself. This paper aims to study the privacy threats contact tracing apps pose through a constitutional perspective. A comparative study is made to analyze the working of contact tracing apps by other countries like the United States and European Union and how they overcome the privacy challenges these apps put forward. This paper also addresses critical recommendations that can be adopted to better implement these apps without any threat to the right to privacy and strike a harmonious construction between Doctrine of Necessity and Right to Privacy.

Keywords: *Contact Tracing Apps, Right to Privacy, Aarogya Setu, COVID-19.*

I. INTRODUCTION

In December 2019, a Novel Coronavirus called SARS-CoV-2 resulted in the outbreak of a respiratory illness that became a global pandemic. Initially, there was no standard treatment for COVID-19, and vaccines were only a farfetched dream. It was essential to avoid infection or further spread. The pandemic led to countries taking drastic measures to contain the virus and prevent it from engulfing humankind. The pandemic made it an all-hands-on-deck situation that the governments used the aid of technology and developed new Digital Applications to contain the virus. Even if the traditional mass testing method took place simultaneously, it was not easy to track other primary and secondary contacts. As smartphones' penetration rate is very high throughout the world, including India, mobile

[1] Author is a Student at School of Law, Christ Deemed to be University, Bangalore, India.

 [ISSN 2581-5369]

phone data could aid public health[2].

The term "contact tracing," for the most part, alludes to recognizing and monitoring people who have been in contact with other individuals who have tested positive to COVID-19, to track and locate other potentially infected individuals. These individuals act as carriers to others, and control measures like isolation and quarantines must be taken to prevent the virus's further spread. Contact tracing is standard protocol in public health investigations and involves officials tracing and contacting infected and potentially-exposed persons. However, with the aid and help of technology, some of the contact tracing proposals aimed at controlling the spread of COVID- 19 suggest replacing traditional contact tracing methods with technology to collect data electronically. These proposals raise questions about how laws governing health information privacy may apply to electronic or digital contact tracing[3].

II. THE WORKING OF CONTRACT TRACING APPS - INVASION OF PRIVACY

In the early days of Covid-19, there was much buzz around contact tracing and the development of contact tracing applications. The concept was a simple one, and your phone would send you an alert if you crossed paths with someone who has been tested positive. These notifications are also called exposure notifications. When you enable exposure notifications, your phone uses Bluetooth to frequently scan for phones in the vicinity doing the same thing. This process runs in the background and therefore reduces the battery consumption. When two phones detect each other, they swap anonymous codes; this code facilitates the phone to record how long you were around the other device and how far from it, which is determined by how strong the signal is. If a person tests positive for covid-19, the health department asks if you'd like to notify other people you are exposed to the virus. On agreement, a code is given to enter into the app; this code will enable your phone to send ID codes to devices nearby, managed by your state or national health authority. In case your phone detects that you have been within 6 feet of a flagged device for more than 15 minutes, it will send you an alert stating that you may be exposed to the virus and what steps to take next.[4]

Effective Contact Tracing consists of three steps

[2] Ranisch, R., Nijsingh, N., Ballantyne, A. *et al. Digital contact tracing and exposure notification: ethical guidance for trustworthy pandemic management.* Ethics Inf Technol (2020). https://doi.org/10.1007/s10676-020-09566-8

[3] Holmes, Eric N.;Linebaugh, Chris D. *COVID-19: Digital Contact Tracing and Privacy Law*. *Hein Online*, 121, (121-129) http://heinonline.org/HOL/P?h=hein.crs/govdauo0001&i=1.

[4] Cat Ferguson, *Do digital contact tracing apps work? Here's what you need to know*, MIT TECHNOLOGY REVIEW (February 4th, 2021, 10:08 AM), https://www.technologyreview.com/2020/11/20/1012325/do-digital-contact-tracing-apps-work-heres-what-you-need-to-know/.

- Identify who is infected
- Identify the people that came in contact with the infected person
- Convince the concerned persons to stay at home.

Evidence suggests that contact tracing apps facilitate in breaking the chain of transmission. Many experts follow national apps of several countries like India, Singapore, Australia, Canada, and Ireland.

Contact tracing apps also include permissions to access location via GPS. The user has provided information like name, age, mobile number, gender, travel history, profession, etc. All this information, including the anonymous code, goes to a centralized database, which is most likely to be controlled by the government or the country's health authority. This raises serious concerns about the transparency and privacy principles adopted to prevent this data's misuse for malicious purposes. India's official contact tracing App, Aarogya Setu, has already been downloaded more than 120 million times, making it the seventh most downloaded app globally[5]. The app collects data and sends it to central servers managed by the government. This information is deleted from the government's database.[6] However, it collects far more data than it is required to collect, the app does not follow the principle of data minimalization. Concerns have been raised by data privacy experts on the app's operating procedure, giving the government an unfair advantage.

III. THE TRADE-OFF BETWEEN PUBLIC HEALTH AND PRIVACY

It is not easy to make a trade-off between privacy Public Health but neither can be sacrificed. In 2017, the Supreme Court of India, in the landmark judgment *Justice K.S. Puttaswamy (Retd.) v. Union of India*[7] held that privacy is an intrinsic part of the right to life and personal liberty under article 21 of the Indian Constitution[8] and was upheld as a fundamental right. Other statutes like Information Technology Act, 2000[9] and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules,) 2011[10], contains specific provisions for the protection of

[5] Dr. Sumeet Kad, *Contact Tracing Apps: Privacy Implications and Trade-offs*, ET HEALTH WORLD (February 4th, 2021, 10:40AM) https://health.economictimes.indiatimes.com/news/industry/contact-tracing-apps-privacy-implications-and-trade-offs/76245542.

[6] Simmhan, Y., Rambha, T., Khochare, *GoCoronaGo: Privacy Respecting Contact Tracing for COVID-19 Management*, J INDIAN INST SCI, **100,** 623–646 (2021), https://doi.org/10.1007/s41745-020-00201-5.

[7] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1

[8] INDIA. CONST. art. 21

[9] Information Technology Act, 2000 (India).

[10] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules,) 2011 (India).

electronic data and lays certain guidelines for entities to comply with to collect, process and store personal and sensitive information of the consumers. These guidelines apply to all corporate entities except certain entities that provide services related to processing sensitive and personal data. Post the Puttaswamy judgment[11], Data Protection Bill, 2019[12], was introduced, and this bill deals with the collection, processing, and storage of all personal data by public and private sector entities.

Aarogya Setu seeks continuous access to location and Bluetooth data. Most contact tracing work on the same principle; however, do not track your location continuously. The issue also arises because the Govt. of India is silent on the highly ambiguous privacy and silence on security practices. The privacy policy of Aarogya Setu is silent on what security practices are being followed to safeguard the citizen's data. More information must be given on what encryption levels are being used and the security practices being followed. There are considerable gaps in India's privacy laws, the Information Technology Act, 2000 and IT Rules, 2011[13] do not require the data processor to make the data subject aware of what is being done with the data. The app also has kept its source code a secret; this means that web and app developers cannot develop a similar app and intends to create a data monopoly.

The contact tracing apps like Aarogya Setu's focal privacy concerns include - Data retention and Location Tracking. The Aarogya Setu App head, Arnab Kumar, backed the app's working by stating that the app was created to match the standard laid down in the Draft Privacy Bill, and the data collected by the app is strictly controlled[14]. However, many ethical hackers and app developers raised many security and privacy concerns after scrutinizing the app when the app was introduced. It should also be duly noted that India was one of the world's first countries that made it mandatory to use the Aarogya Setu app to specific containment zones. Another paramount concern is that personal information "secured" by the app includes an individual's profession, which has no connection with the app's working whatsoever. The definition of anonymous data is not clear, especially until the app will retain its data. Other privacy and security concerns include the sharing of data with third parties. Data shared on the app can be reshared to different branches of the disaster management authority. However, it was assured by the Ministry of Electronics and IT that the health

[11] *supra* note 6
[12] Data Protection Bill, 2019 (India).
[13] *supra* note 8.
[14] *Aarogya Setu: Lack of Data Privacy Laws, Transparent Policies Make App Worrisome, Say MIT Researchers*, First Post (February 5th, 2021, 1:45PM), https://perma.cc/E3S5-TUQE

 [ISSN 2581-5369]

institutions would only share the data to other departments of health when it is strictly a necessity to frame/implement appropriate health responses[15].

According to the Puttaswamy judgment, the Supreme Court laid down a threefold prerequisite that must be followed to justify the invasion of privacy -

1. A Legal Backing

as legal packing the government in the national disaster which empowers the government to take all essential and necessary measures which give an exemption to any privacy violations; however that for the use of the contractor racing app, there must be a legal framework in place to protect the privacy and prevent health surveillance from turning into mass surveillance by the government and cannot use the national disaster management act as a legitimate legal backing for rolling out this contact tracing app which violates the fundamental right to privacy

2. Necessity - Legitimate Aim

The government's main aim for releasing this contract tracing app, Aarogya Setu, is to contain and track the covid-19 virus. This app becomes effective only if most of the population use a Smartphone and actively use the app. It is also to be noted that the accuracy is not proved to be reliable. it is wholly understood the government is trying to leave no stone unturned to contain the virus, but it must also be taken into consideration that the excuse of necessity can be taken only if there is an effective and proven mechanism for which the right to privacy is being compromised

3. **Proportionality and Rational Nexus**

The rationale stated by the government is not very convincing when it comes to putting the right to privacy in jeopardy when the accuracy of the whole app is in question. The terms and conditions of the Aarogya Setu app have a clause that takes away the government's liablibity for the false identification of the virus and inaccurate infected individual data. Other provisions like resharing data to other health departments for administrative and research purposes cannot take the defense of necessity and definitely do not pass the proportionality test[16].

[15] Patrick Howell O'Neill, *India Is Forcing People to Use Its Covid App, Unlike Any Other Democracy*, MIT Technology Review (February 5th, 2021, 4:05PM) https://perma.cc/Q5ZS-VZSL

[16] Vakasha Sachdev, *Does Govt's New Data Protocol Address Concerns over Aarogya Setu?* The Quint, (February 4th, 2021, 10:40AM), https://perma.cc/KM2E-R8BR

 [ISSN 2581-5369]

IV. COMPARITIVE STUDY WITH OTHER COUNTRIES

The right to privacy is considered a fundamental human right under Article 12 of the Universal Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights. The United Nations General Assembly resolution 68/167 safeguards this right as it compels the states to respect and protect the right to privacy, including in the context of digital communication' by reviewing their procedures, practices, and legislation regarding the surveillance of communications, collection of personal data, etc.

The European Union

The European Union has one of the most stringent data protection laws globally in the form of the EU General Data Protection Regulation (GDPR)[17]. The GDPR defines personal data as any information relating to an identifiable natural person ('data subject'), in particular reference to an identifier such as name, an identification number, location data, an online identifier, or specific details about the genetic, physical, mental or social identity of that person. The data that is stored in the smartphone of an individual is information related to the individual. Even if it is encrypted, the unique identifiers broadcast could be linked to natural persons. There is an excellent chance these encrypted codes come within the ambit of 'information' related to an individual and therefore meet the definition of personal data under GDPR if the agencies can identify the person with this information, like the person's primary contact who has been tested positive.

Apple and Google, with their respective contact tracing systems, made it clear user data broadcasted through their Exposure Notification Software (ENS) has been anonymized. However, data anonymization is still a moving target legally. The European Data Protection Board (EDPB) has set a very high bar for data anonymization, and data controllers usually cannot match these standards.[18] There is significant research that shows there exist several re-identification techniques using anonymized information.

Therefore, based on the currently available information, all kinds of contact tracing apps are a personal data processing system and shall be subject to the regulations under GDPR. Article 24 of the GDPR states that data controllers should implement proper technical and organizational measures to ensure that all data processing occurs according to the principles

[17] Klonowska, Klaudia, and Pieter B. *The COVID-19 Pandemic: Two Waves of Technological Responses in the European Union*. Hague Centre for Strategic Studies, 2020, (February 5th, 2021, 4:05PM) www.jstor.org/stable/resrep24004..

[18] Laura Bradford, Mateo Aboy, Kathleen Liddell, *COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes*, *JOURNAL OF LAW AND THE BIOSCIENCES*, Volume 7, Issue 1, 2021, https://doi.org/10.1093/jlb/lsaa034.

highlighted in Article 5 of the GDPR. The principles are:

- Lawfulness, fairness, and transparency.
- Purpose limitation.
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

These principles call for a specific architecture of protection and enforcement. The GDPR mandates certain pre-defined rights of the individuals or 'data subjects,' including the right to rectification, right to erasure, and access. To ensure proper enforcement of the same, the Member State assigns a competent authority to oversee the same operation. Data controllers must also conduct specific impact assessments and risk mitigation measures. In the European Union, the data subjects have the right to seek judicial remedies and to receive compensation.

The United States

US Privacy laws such as the Health Insurance Portability Act (HIPAA) or the CCPA 2018 to a proximity tracking system is more limited. This lack of coverage might seem to encourage innovation, but there is a greater risk that the absence of comprehensive standards could undermine public trust. HIPAA's privacy rule only applies to data collected by health providers or businesses hired by health providers to process their data. An individual's diagnosis from a diagnostic lab would, therefore, be subject to HIPAA's privacy rule, but a Bluetooth exposure proximity system does not fall under HIPAA. As long as the individuals are giving information to the contact tracing app and not the health provider directly, HIPAA won't be applicable.[19] This regulatory gap may facilitate some innovation in the contact tracing and tracking software space. However, with some being less trustworthy and reliable than others, several products could cause hindrances in the adoption of reliable contact tracing apps. [20]

[19] Carmel Shachar, *Protecting Privacy in Digital Contact Tracing for COVID-19: Avoiding a Regulatory Patchwork*, HEALTHAFFAIRSBLOG, https://www.healthaffairs.org/do/10.1377/hblog20200515.190582/full/

[20] *Cf.* Jack Morse, *North Dakota Launched a Contact-Tracing App. It's Not Going Well*,MASHABLE UK, https://mashable.com/article/north-dakota-contact-tracing-app/?europe=true

The California Consumer Privacy Act

The CCPA is a consumer protection statute. By its terms, it excludes data covered by the HIPAA and other state laws concerning the privacy of medical information. Furthermore, the CCPA does not apply to small businesses unless their primary business income comes from data brokerage. Also, the CCPA has lower standards of anonymized or de-identified information, and therefore it is likely that the encrypted Bluetooth signals might be classified as 'de-identified' under the CCPA.

V. RECOMMENDATIONS

We cannot put a definite deadline as to when the pandemic might end, and we still need technology to combat the virus. If the contact-tracing apps could be regulated and re-modeled into a secure app upholding all privacy guidelines, this app could be a pioneer in the COVID-19 battle. We can take inspiration from different contact-tracing apps by the private sector and other countries to examine how the privacy issues have been overcome.

- The contract to a contact-tracing app developed by Singapore-trace together uses a dynamic ID, which adds an extra layer of security and upholds anonymity. India can use this feature in the Aarogya Setu App instead of using a static ID and could prevent collecting many unwanted data from its users. Dynamic ID prevents the app from being vulnerable to De-anonymity[21].
- Proximity data should be used as an alternative to location tracking. Hence the use of GPS and location data could be limited.
- The app must have an option to let the users delete all the data when they no longer want to use the app. This will prevent data retention in the central server and cannot be reshared to other unauthorized sources.
- Stanford's COVID-Watch app has a feature that generates an anonymized heat map to indicate high-risk areas[22].
- A board must be established to monitor all electronic and digital applications in COVID-related projects.
- A complaint mechanism must be set up to report any breach of privacy arising due to the act.

[21] Shreyasi Singh, *Contact Tracing applications to monitor COVID-19: The Aarogya Setu app and the Right to Privacy*, Bar & Bench, 2020, https://www.barandbench.com/apprentice-lawyer/monitoring-covid-19-right-to-privacy-amidst-contact-tracing-applications

[22] *Id.* at 23.

- A transparent mechanism must be established to establish that the government has acted following all protocols to protect privacy. This helps to gain the trust of the users and increases the integrity of the app.
- Making de-centralized apps is better than a centralized-controlled app to uphold privacy policies. In a centralized approach, data protection and data storage can jeopardize the trust of the public due to the privacy challenges that it poses. Many countries like Germany and The United Kingdom have adopted de-centralized contact-tracing apps.

VI. CONCLUSION

No doubt that Aarogya Setu and other local contact-tracing apps have played a paramount role in tracking and containing the virus, spreading like wildfire across the globe. A new and improvised version of such apps, which have improved privacy-protection protocols, would only be an asset. If the contact-tracing apps should be a huge success, then pubic trust and confidence play an essential role in protecting individual privacy. There must be a harmonious construction made between the necessity of public health and the right to privacy. The COVID-19 pandemic and the implementation of contact-tracing apps should be taken as an opportunity to identify the loopholes and vacuums in the privacy laws in our country. Laws that protect all kinds of electronic data, even during an emergency or gross necessity, must be implemented so that privacy is not sacrificed to accommodate other necessities.

*****

 [ISSN 2581-5369]