SUPREMO AMICUS

VOLUME 24, MAY 2021 ISSN 2456-9704

CONTACT TRACING APPS OF COVID-19 VIS-A-VIS PRIVACY ISSUES: A STUDY

By Dr Amita Verma, Associate Professor, University Institute of Legal Studies, Panjab University

By Dr Karan Jawanda, Assistant Professor, University Institute of Legal Studies, Panjab University

Abstract

Surveillance is not a new concept for the Government agencies of any country but during COVID-19 pandemic it gives an extra wing to government agencies to do digital surveillance. Digital Surveillance has been done with the help of interfaces to allow bluetooth or location tracking or contact tracking methods using Android or iPhone communication devices. During the COVID-19 outbreak the government agencies of China, Singapore, India, Israel etc. are using contact tracing apps for COVID-19 patient and helping the society against the COVID-19 virus. This technology is helpful for tracing the contact of certain geo-location area and breaks the chain of strain of virus.

But it raises many question before all of us- What about the right to privacy of the Individuals who are downloading these apps?, how their data has been stored?, where it has been stored?, is our data in encrypted form?, is our data protected? What are the methods to destroy our data after this pandemic is over? Etc. This paper shall deal with the problem and issues relating to privacy because of contact tracing apps for COVID-19, the need for data protection, comparative analysis of different apps being used by different countries with respect to privacy and data protection. The paper shall also outline the legal provisions relating to surveillance and interception of data under Indian Telegraph Act and Information Technology Act 2000 along with rules. Findings and suggestions regarding the issue shall also be discussed.

Keywords: Digital Surveillance, Contact Tracing, COVID-19, Interception and monitoring of data, Privacy issues

Contact Tracing Apps of Covid-19 vis-a-vis Privacy Issues: A Study

Introduction

Year 2020 has changed the thinking of every individual on this planet; this is all because of one virus known as CORONAVIRUS or COVID-19. It has changed and impacted us socially, economically, physically as well as mentally. Within the past year, the Covid-19 pandemic has greatly impacted each aspects of human life including socio-political scenario. It has added a new dimension to concept of privacy and affected protection of personal data and information. The pandemic has made it necessary to bring about a balance between our fundamental rights like privacy on the one hand and health and security on the other hand.

COVID-19 crisis is more severe as compared to previous pandemics like Spanish Flu or Asian Flu. Governments of various countries are taking all measures and precautions to combat the spread of this menace. The WHO has emphasized the role of contact tracing as one of the pillars to check the rate at which the COVID-19 pandemic can spread. The usual mode for contact tracing is physical and manual. However, where physical and manual tracing can be time- consuming and

cumbersome, technology based digital tracing comes in as a handy solution. Digital tracing helps to effectively trace people who may have come in contact with people who positively tested for COVID-19. The whole idea is to break the chain of infected people from coming into contact with healthy individuals and provide for timely isolation or quarantine of such persons. In order to achieve this objective, many countries have launched the tracking or surveillance apps to fight against this pandemic. Digital tracing/tracking is undoubtedly an effective measure to curtail the spread of this pandemic but it raises serious issues like infringement of privacy and data protection.

Digital Tracing apps and digital tracking system has played a main role for surveillance of people after the outbreak of COVID-19. Many big IT giants[1] gave hands to public health authorities for making such application software which perform the contact tracing by the use of cell phones having IOS or Android operating system. But it raises a very serious question before the world about the protection of privacy of an Individual. Whether the Government can do large scale contact tracing without infringing the privacy of an individual which is protected under Constitution of India and upheld by the Supreme Court in the case of Justice K.S.Puttaswamy (Retd) v Union of India[2]. The right to privacy is also protected under GDPR and OECD Privacy Guidelines[3]

Contact Tracing Apps by Various Countries

Many countries were also working on application software which aimed to facilitate the battle against the COVID-19 catastrophe. These application software either based on geo-location or Bluetooth technology also known as digital handshake. Examples are StopCovid19 in Spain, Stopp-Corona App in Austria, StopCovid in France, ProteGo in Poland and Aarogya Setu App in India. In April 2020, Indian Government also launched Aarogya Setu App[4] for COVID -19. The US government is not currently requiring their citizens to download any tracking apps.

Open source Image[5]

Common Features of these Apps are updates of confirmed cases, real time location based monitoring, home isolation and quarantine

[1]https://www.apple.com/in/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology visited on 19/2/2021

[2]https://indiankanoon.org/doc/127517806 visited on 11/2/2021

[3]The OECD's Privacy Framework at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdfvisited on 19/2/2021

[4]https://www.aarogyasetu.gov.in/ visited on 11/2/2021

[5]https://www.forbes.com/sites/niallmccarthy/2020/07/22/which-countries-are-deploying-coronavirus-tracing-apps-infographic/?sh=573d11c46d34 visited on 19/2/2021

monitoring system, self reporting symptoms, need of doctor alert, sample alert, direct reporting to government or public health department and general awareness about COVID-19.

Basically it is a contact tracing, syndrome mapping mobile based app or digital service for helping health departments to identify COVID-19 clusters but it also raises privacy and security concerns. These apps track the information using Bluetooth technology or geo location because of interoperability of the devices.

Contact Tracing by India

India is using The Aarogya Setu App which was a replacement for an earlier app known as the Corona Kavach[6]. The app in India is developed by the National Informatics Centre jointly with NITI Aayog. The app aids the frontline health workers in identifying hot spots and accordingly take preventive measures. Its main purpose is to create awareness among the users about COVID-19 and update them about the health services provided by the healthcare sector to protect the people of the country from this pandemic.[7] The Aarogya Setu app is the contact tracing device which uses the GPS or Geo-location or Bluetooth technology for tracking the infection by taking the data from the users or updating the data of the confirmed cases of the COVID-9 patients. By this app people are able to know that from their location within six feet who all are the COVID infected patients and then they take the precautions accordingly. This app also provides location of the infected or hot spot area of COVID as declared by the authorities based on the data.[8]

Aarogya Setu has some features on its app like User status which tell the user about his own risk of contracting COVID-19, then another feature is about self-assessment which helps the users to identify his symptoms of COVID-19 and take the help of the public health department or self-quarantine then another feature is in relation to COVID-19 updates locally or globally. This app also tells about the number of COVID-19 cases in a particular radius or area and increase or decrease of the number of cases in India.[9]

The Central Government made it mandatory for all employees to download the app on their mobile phones on 29 April 2020.[10] But later, there was serious criticism of this app and it was termed as a "sophisticated surveillance system" as it is not backed by any law and questioned "under what law, government is mandating it on

[6]https://www.financialexpress.com/industry/technology/govt-discontinues-corona-kavach-aarogya-setu-is-now-indias-go-to-covid-19-tracking-app/1919378/ Visited on 19/2/2021.

[7]https://www.livemint.com/technology/apps/govt-launches-aarogya-setu-a-coronavirus-tracker-app-all-you-need-to-know-11585821224138.html visited on 19/2/2021

[8]*Ibid*

[9]"Aarogya Setu announces Bluetooth proximity feature for contact tracing! Here's how to check", https://www.financialexpress.com/industry/technology/aarogya-setu-announces-bluetooth-proximity-feature-for-contact-tracing-heres-how-to-check/2014917/ visited on 19/2/2021

[10]"Centre makes Arogya Setu app must for all central govt employees", https://www.indiatoday.in/india/story/centre-makes-arogya-setu-app-must-for-all-central-govt-employees-1672415-2020-04-29 Visited on 19/2/2021.

anyone".[11]However, on May 26, 2020 the Government made the source code of the Aarogya Setu App public.[12]

However, there have been some concerns regarding the Aarogya Setu app. The aarogya setu privacy policy provides that the all personal information collected at the time of registration will be retained till the account remains in existence[13]however, there is no clear way for users to opt out. It is unclear if deleting the app amounts to cancellation of registration. The purposes for which the personal data will be used by the government should also be made clear. It should not be used to make profit. Also, doubts have arisen as to its use after the pandemic. This is because the NITI Aayog has indicated that it will form the basis for building the National Health Stack.[14] In absence of a Personal Data Protection legislation, the scope of Aarogya Setu app should not be expanded except for checking the Covid-19 pandemic.

Problems associated with Contact Tracing Apps

The two main companies, Google and Apple have announced that they will work together so that they can uses technology to detect exposure to people having Covid-19. They are using technology of mobile devices and Bluetooth communications protocol. These protocols contain the exposure notification which changes the key of the device after every 10 to 20 minutes. But certain countries are not using the Apple or Google contact tracing apps which are dealing with notification protocol but other apps which have failed to implement strong security measures to protect the privacy and data of the individual while tracing the covid-19 patient.

More than 50 countries are developing COVID-19 Contact tracing apps to combat the COVID-19 crisis to carry out mass surveillance on the people and with the help of mass surveillance identifying the infected people who have a strain of this virus. But many people have raised their voices and are concerned regarding the right to privacy of an individual. For example, China collects their citizens' complete identity, location and online payment modes etc without their consent.[15]

These contact tracing apps can have access to users' mobile devices and collect various types of data of the users. For example, they have access to all contact lists, all photos, media files, location, any change of location, Camera, device ID, call information, WiFi connection, microphone, network access, Google service configuration, network and audio settings, so on and so forth. They also have an information of the users as per the information collected by the app such as name, age of the user, email id, phone number, postal address postal code, device location, unique ID, mobile IP address, operating system of the device, IP address, types of browser used on the device etc. Governments are claiming that the personal data or information of the users are

[11]"Mandating use of AarogyaSetu app illegal, says Justice B N Srikrishna", https://indianexpress.com/article/india/aarogya-setu-app-mandate-illegal-justice-b-n-srikrishna-6405535/visited on 19/2/2021

[12]Nic-delhi/AarogyaSetu_Android, nic-delhi, 27 May 2020, visited on 12/2/2021

[13]http://www.aarogyasetu.gov.in last visited on 20.05.2021

[14]http://orfonline.org/expert-speak/aarogya-set-app-many-conflicts-67442/ last visited on 20.05.2021

[15]*Supra* 5

anonymous, encrypted and secured and such information related to people not tested COVID positive will be destroyed from the server 45 days after being uploaded and who is tested positive their information will be removed from the server 60 days after such persons have been declared cured of Covid 19.[16] The privacy policy of aarogya setu has been changed to the effect that the data will not be shared with third parties. Now the question arises whether all such personal data of the individual which was collected by these apps are protected by any laws or regulation locally or globally and nationally or internationally or not?

The fact is that, these apps are continuously monitoring and intercepting and doing surveillance and also collecting and processing the highly personal identifiable information or sensitive personal data of an individual such as health information, location and direct identifiers such as name, age, email id, nationality etc. Thus, it becomes questionable as to how the government will use this data. There could be a chance of misuse of data as the government has complete information about the individual including his/her entire social network.

Privacy Issues

The European Data Protection Board emphasized the need for protecting personal data during the fight against COVID-19 and issued legal regulations for processing personal data with reference to epidemics under the General Data Protection Regulation.[17]

In India, the Supreme Court has upheld the Right to Privacy as a fundamental right[18]and the same is protected under Articles 14, 19 and 21 of the Constitution of India, being incidental to other freedoms guaranteed by the Indian Constitution. It also states that there was a need to introduce a data protection regime in India. But on the other hand, Information Technology Act 2000 provides surveillance and Interception of data. In India, the Indian Telegraph Act, 1885, provides for interception of calls, and the Information Technology Act, 2000 alongwith certain rules, deals with interception and monitoring of data by the Government to conduct surveillance.

According to GDPR, any information that is broadcast by devices and later collected by any app, is considered to be personally identifiable information as per Article 4 of GDPR. The IT companies are claiming that they are not tracking and keeping the location data for Bluetooth and keeping the privacy at first level but they somehow won't be able to

[16]Rao, Rajiv. "India's contact tracing app made open source, but will this thwart a surveillance state?" https://www.zdnet.com/article/indias-contact-tracing-app-made-open-source-but-will-this-thwart-a-surveillance-state/visited on 19/2/2021, and also https://www.aarogyasetu.gov.in/privacy-policy/#:~:text=The%20App%20is%20equipped%20with,in%20a%20secure%20encrypted%20server visited on 25.05.2021

[17]https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-datacontext-covid-19-outbreak_en;http://covid19.who.int?gclid=Cj0KCQiA4L2BBhCvARIsAO0SBdbp2D4gSjGydgTSY9vn0B1B3YOMDGsDV33t5HZnMQ4JZfz5VgXnuMaAk1NEALwwcBvisited on 19/2/2021

[18]Justice K.S. Puttaswamy(Retd) vs Union of India available at https://indiankanoon.org/doc/127517806 visited on 11/2/2021

separate or disassociate the data completely and remain subject to the GDPR.[19]

Extra protection is needed under GDPR in case information is related to health of the user. Even in India, in case of Sensitive Personal Information of the user extra precautions are needed and protection like liability under Section 43A of the Information Technology Act, 2000 along with IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. But Government has no liability under Section 43A of the IT Act.

After the amendment in the year 2008 of IT Act 2000, unprecedented powers have been given to both Central and State Government of interception, monitoring, decryption and blocking of all the electronic data and information generated, transmitted, received or stored in any computer, computer network, computer system and computer resource under Section 69, 69 A, 69 B, and 29.

Section 69A and 69B has provided various grounds such as security, sovereignty and maintaining public order etc under which Central Government and State Government has a power to monitor any electronic communication which is passing through any electronic resource in India.

Along with this, there are rules of Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 which states that there is a need to take approval for monitoring any data or information from the competent authority.

In the case of Shreya Singhal vs Union of India[20] the Supreme Court of India, examined the constitutional validity of various provisions of the Information Technology Act, 2000. Section 66A of the Information Technology Act 2000 has been declared unconstitutional but *Section 69A and the Information Technology (Procedure & Safeguards for Blocking for Access of Information by Public) Rules 2009 and* Section 79[21] has been upheld.

If we look at GDPR governance, processing of personal data needs "lawful basis" and if involves health data also then need strict threshold for the same. But in case of Contact tracing apps of COVID-19 made by private companies for the Government of their respective countries involves public private collaboration. This Public Private handshake raises interesting question with regards to privacy and data protection. As private big IT giants are involved no doubt for helping the government in the time of crisis but whole data has been outsourced by the respective government in the hands of these companies. In this way it really loses the public trust.

For example in China, Some companies like WeChat or Alipay, are hosting the Health Code App which is tracking the corona virus exposure, health data etc. but they have asserted rights under contract that they will

[19] GDPR Recital 26;Whitaker&Etherington,supra note 5 (admitting that even with the privacy controls Google
and Apple could hack the system to obtain access to personal data).

[20](2013)12 SCC 73

[21]http://www.livelaw.in/summary-of-the-judgment-in-shreya-singhal-vs-union-of-india-read-the-judgment/visited on 19-2-2021

keep the data of the users after the crisis is over.[22]

One more issue relating to COVID-19 is that many countries do not have any technological solutions to this pandemic and if any person travels cross border then issue arises again how to know he is COVID carrier or not? What to do if he is a carrier of COVID-19 But no warning has been issued to the cross border country for self isolation, or home isolation of such patient as these apps are locally not globally connected.

In case of contact tracing they are not only taking general information of the user but taking health related information as well, which attract Article 6 and 9 of the GDPR. Article 6[23] of the GDPR needs legal basis for the processing of personal information or data of the user and Article 9 deals with the processing of special data such as health related data which is forbidden under the GDPR unless specific exemption applies as it needs separate permissible basis. In case of Covid-19, the lawful basis is to protect the public from the Corona virus pandemic by using the COVID-19 Contact tracking apps. And public has a choice to download or delete the app. But whoever is giving their consent the same is not considered to be freely given due to the power or potential power of public authorities.[24]European authorities make it clear that voluntary use is important safeguard under the GDPR even if consent is not relied upon as lawful basis.[25] Even under OECD principles[26] requires consent in case of personal data undertaken. As such consent is required under GDPR for data storage and lawful basis, no doubt for public authorities there is no need of consent but it be sought as a safeguard where possible.[27] Consent of user is also required in case of EU e-privacy Directive for protecting mobile data services or network.[28]

But in case of China and Israel users consent is not taken by public authorities as in users mobile phones virus tracing software

[22]Remarks of Ruipeng Lei, Huazhong University of Science and Technology, Wuhan, China, Beyond the Exit Strategy:Ethical Uses of Data-Driven Technology in Fight Against COCID-19, Nuffield Council on Bioethics and Ada Lovelace Institute Webinar, https://www.nuffieldbioethics.org/publications/covid-19/webinar-beyond-the-exit-strategy-ethical-uses-of-data-driven-technology-in-the-fight-against-covid-19 visited on 19/2/2021

[23] GDPR Art. 6,"The CCPA does not set a list of grounds that businesses must adhere to a priori to collecting, selling and disclosing personal information, and only provides for a posteriori mechanism, namely allowing customers to opt-out to the sale and disclosure of their personal information or to ask for erasure of the information."

[24] Letter from Andrea Jelinek, to Olivier Micol, (stating that consent is not the most relevant basis for use of tracing apps by public authorities); EDPB Guidelines (stating that Art. 6(1)(e) task in the public interest appears to be the most relevant legal basis).

[25] Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, 4, https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7 (accessed Jan. 28, 2020); Guidelines 04/2020 supra note 32 at ¶¶8, 24, 31.

[26] 3 OECD Guidelines on Principles on the Protection of Privacy

[27] The GDPR also provides data subject the right to object to processing of their data on a public health or other Article 6 basis. GDPR Art. 21

[28] Council Directive 2002/58 art. 5(3) 2002 O.J. (L 201) 37 (EC) [hereinafter ePrivacy Directive]. As is the case under the GDPR, processing done on the basis of Member legislation that constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard public security may be undertaken without consent. ePrivacy Directive Art. 15. See also EDPB Guidelines 04/2020 supra note 32 at ¶¶ 10–13.

automatically installed and do surveillance.[29] Even in India Government had issued a mandatory order or condition for the government employees to install contact tracing app on their mobile phones before returning to workplace or before joining the office after lockdown was over.[30] But in India they have the privacy policy which says that they will retain data for 45 days or 60 days in case of personal data of people. But have no mention as to what they will do after that? How will they destroy that data?

Thus many questions still remain unanswered like will contact tracing apps really help in a mass scale monitoring phenomenon during COVID-19? Whether these apps help us in any way to combat the COVID-19 crisis? There are going to be certain fundamental issues and challenges such as, how the government is going to be transparent?, who will be authorised to collect data?, what data will be collected?, how it will be used?, and how the right to privacy will be protected?

Conclusion

No doubt, Contact tracing is the need of the hour for all over world to curb the COVID-19 crisis. But at the same time Privacy and security issues also need and demands protection. And for that voices are raised from various stakeholders for developing the protection mechanism that may be useful also. Such as, some are saying that we should identify tracing protocols that mitigate privacy risks and promote the use of critical security and privacy controls that can accelerate medical responses while maintaining people's rights[31]. Others are proposing a system for secure and privacy-preserving proximity tracing at large scales through the application of anonymous identifiers and functional requirements of fundamental security and privacy, such as data minimization and retention[32].

Public health authorities must take all possible measures to protect the lives of millions and millions of people and combat the spread of virus and for that they do need steps like mass surveillance through contact tracing apps. The next job is of the workers from IT Sectors or those who are associated with the Information Privacy and security Departments, to see what they can do to protect the privacy and data security. Thus, Government along with the IT Sectors must develop good polices and technological measures to protect the data which may be personal data or sensitive personal information of the user for promoting transparency and ensuring the protection of

[29] See Natasha Singer & Choe Sang-Hun, As Coronavirus Surveillance Escalates, Personal Privacy Plummets, NY Times (Mar. 23, 2020); Helen Davidson, China's coronavirus health code apps raise concerns over privacy, The Guardian (Apr. 1, 2020).

[30] Coronavirus Lockdown: No More Voluntary, AarogyaSetu App Now Mandatory for Office Workers, https://www.indiatoday.in/technology/news/story/coronavirus-lockdown-no-more-voluntary-aarogya-setu-app-now-mandatory-for-office-workers-1673438-2020-05-01
TheMinistry of Home Affairs has backed away from this stance and instead suggested that citizens use "best efforts" to use and install the app. Privacy Activists Pleased as Centre Soften Stance on AarogyaSetu App, New Indian Express, https://www.newindianexpress.com/states/telangana/2020/may/19/privacy-activists-pleased-as-centre-softens-stance-on-aarogya-setu-app-2145222.html visited on 19/2/2021

[31] Hart, V. et al. Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 while Mitigating Privacy Risks (Edmond J. Safra Center for Ethics, 2020).

[32]Troncoso, C. et al. https://github.com/DP-3T/documents (2020) visited on 19/2/2021

civil liberties. Stress should be laid on anonymization of data, consent based adoption of apps, controller of contact tracing apps should be defined so that liability in case of misuse can be fixed, data should not be used for any other purpose except Covid-19 management and principle of data minimization and data protection by design and default should be implemented.

Ultimately, it can be said that the success of these apps will depend on several parameters like the number of persons among a population who install it, access of general public to technology like mobiles etc, meaning of a contact and his duration of closeness, honest self-declaration of users regarding their health conditions, accuracy of information to users and usefulness of consequent alerts to public health system, strict adherence to the rules as per GDPR and the "e Privacy Directive" regarding using personal data of individuals. Moreover, emphasis should be only on monitoring the contacts of an individual rather than tracking the movements of the individuals. Countries must issue or frame laws/ rules and regulations regarding rights and obligations of all parties involved in contact tracing inspite of obtaining consent from the users. Only with a proper legal framework ensuring checks and balances, we can hope that contact tracing apps which definitely involve digital health surveillance can be successful tools to control the pandemic.

*****