# DATA PRIVACY IN COVID-19 WORLD: CONTACT TRACING APPLICATION

—*Aparna Singh*[*] & *Akanksha Pathak*[**]

*Abstract*—*In today's world individuals are connected on a large scale through various apps and devices. Their acts are linked through different networks and platforms. From computers to mobile to the wrist watch of an individual, all are hyper-linked to collect various data which is constantly being monitored and analysed by different authorities. In present time with the impact of ever-increasing cases of covid-19 in all over the world many countries have evolved various methods to control the spread of the virus and one such feature is contact tracing apps like AroygyaSetu. Different contact tracing apps have been implemented which collects large scale aggregate data for yielding valuable results which can improve in the public health sector by creating more tools for its transformation and expose the new avenues and discovery in the sector. On one hand these apps and hyper- linked world give better results in our daily lives from communication to travel but on the other hand hyperlinked world has made our privacy a slack by monitoring our every move. Thus these contact sharing apps have provided a potential threat to our privacy on the presumption of making society a better place. This contact sharing app takes various data of an individual which is often shared with different third party servers and is often leaked online which puts into danger the privacy of various individuals. In India in the absence of any well-defined data protection law and the government laying out these apps and making it mandatory at many places which use personal data of an individual often put the collected data into speculations of misuse and a threat to individual data privacy.*

[*] Ph D (Law), Assistant Professor of Law, Dr. Ram Manohar Lohiya National Law University, Lucknow. <greeneyeaparna@gmail.com>.

[**] Research Scholar (Law), Dr. Ram Manohar Lohiya National Law University, Lucknow.

**Keywords:** Data privacy, Right to privacy, Contact tracing apps, Data protection law, Privacy policy.

## I. INTRODUCTION

Covid-19 pandemic has been dominating the whole world. It has created a global health emergency in all the countries and has outlined various flaws and weaknesses not only in the public health system of the countries but others also. Pandemic is creating a large impact on various other sectors of the countries like technology, travel, food and business, which has in turn shattered the economies of the country[1]. Thus to stop the spread of the virus in all over the world, various measures have been taken by all the nations, from lockdowns to closing of flights and international border but then also the spread of the virus could not be controlled which has ghastly engaged all the sharp minds to develop further measures to control the pandemic and one such way was the development of contact tracing app. Contact tracing app uses different methods to inform people who may have come in contact with the one who has tested positive for the virus in recent days and to take prompt methods like isolation and medications to stop the spread of virus.[2] Nowadays our whole life has been hyperlinked by various apps from our mobile phones to digital watches. Our every move is being monitored and analysed by the apps which collect data, synthesize and analyze to make more advanced technologies capable of understanding human actions.

## II. CONTACT TRACING TECHNOLOGY

Contact tracing is not a new phenomenon, in the past manual contact tracing has been used severely by various nations to stop the spread of infectious diseases such as HIV, SARS and Ebola.[3] Given the nature of Covid-19 infection which is spreading rapidly as on 4th August, 2021 there has been 199,466,211 confirmed cases of Covid-19 and 4,244,541 people have died so far due to the infections.[4] Thus, the rate of spread of Covid-19 virus is fast mov-

---

1 Joe C. Mathew, "2,395 Companies Shut Down in Delhi in Apr 2020-Feb 2021; 1,936 in UP, 1,322 in Tamil Nadu" <https://www.businesstoday.in/latest/economy-politics/story/10113-companies-shut-down-in-india-from-apr-2020-feb-2021-delhi-tops-the-list-290397-2021-03-09> (last visited 17 October 202).

2 "Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 While Mitigating Privacy Risks", Harvard University Edmond J. Safra Center for Ethics, <https://ethics.harvard.edu/outpacing-virus> (last visited 16 October 2021).

3 *Ibid.*

4 WHO Coronavirus (Covid-19) Dashboard, <https://covid19.who.int>.

ing if compared to other such viruses. So for stopping the spread of the virus manual contact tracing cannot be as fruitful as it has been in the past given the time and man force taken to collect the manual data and small period of incubation of Covid-19 that, in the span of 11 days over 95 percent of people have developed symptoms[5] and similarly the share of asymptomatic patients are 15 to 56 percent.[6] With the over empowering dependence of technology in our daily lives, advanced technological surveillance has become a way or as an alternative to manual tracing of people, who have contracted virus or have the symptoms of Covid-19 and tracing individuals who have come in contact with the positive tested patients.[7] Thus digital contact tracing is an advanced technological solution which helps in recognising and detecting individuals who have been in proximity with another persons who has been diagnosed and exposed with contagious Covid-19 Virus.[8] These apps further help in locating the other proximate people quickly and give guides to take measures and medical help to prevent the spread of contagious virus.[9] Various nations and companies have deployed these apps like Singapore Trace Together, Indian Arogya Setu and Brazilian SIVEP Gripe etc. These apps work on the primarily two technologies one is GPS and other Bluetooth and few apps use a combination of both.[10] When two devices pass closely from one another, radio waves are emitted from the devices which are captured as a wave by the other device within a specific range and time which is known as "Bluetooth Handshake".[11] Contact Tracing Apps collects data of a user over certain time limits which is processed and analysed over time in a centralised or decentralised server. Under centralised server data from user phone or Bluetooth device is stored on a centralised server of the government whereas as in decentralised server data is stored locally on the individual device until and unless that individuals has been tested positive or has any symptoms, which then sends data to the server

---

5 Stephen A. Lauer et al., "The Incubation Period of Coronavirus Disease 2019 (COVID-19) From Publicly Reported Confirmed Cases: Estimation and Application", 172 Annals of Internal Medicine, 577 (2020).

6 Kenji Mizumoto et al., "Estimating the Asymptotic Proportion of Coronavirus Disease 2019 (COVID-19) Cases on Board the Diamond Princess Cruise Ship, Yokohama, Japan, 2020", 25 Eurosurveillance,(2020).

7 Divya Ramjee, Pollyanna Sanderson and Imran Malek, "COVID-19 and Digital Contact Tracing: Regulating the Future of Public Health Surveillance", 2021 Cardozo L. Rev. De-novo, 101 (2021).

8 Sacha Alanoca et al., "Digital Contact Tracing Against COVID-19: A Governance Framework to Build Trust", 11 International Data Privacy Law 2021, 3 (2021).

9 Eric N. Holmes and Chris D. Linebaugh, "COVID-19: Digital Contact Tracing and Privacy Law", 2020, 1(2020).

10 Samuel Woodhams, COVID-19 Digital Rights Tracker (Top10VPNResearch) (March 20, 2020), <https://www.top10vpn.com/research/investigations/covid- 19-digital-rights-tracker/> accessed 11 October 2020.

11 Leo Kelion and Rory Cellan-Jones, <https://www.bbc.com/news/technology-54250736>, last visited September 24, 2021).

which is searched by other users data who have come in the contact with that positively diagnosed individual[12]

## III. HOW DOES THE APP WORK?

Contact Tracing Apps have been laid down by different entities, in some countries government departments have laid down these apps like Indian Arogya Setu App has been built by Ministry of Information and Technology[13] whereas in some countries are dependent on private organisations like Google and Apple to make such apps[14] When you download these apps there is certain information being asked like name , age , phone number, which is taken and stored on a digital server which can be centralised or decentralised and a unique digital id is created of such a user in the app which is used for further identification by the app.[15] Some apps even go on asking for more detailed information and their surveillance is also very stringent which has created certain concerns in minds of individuals using such apps. In Aarogyasetu app unique digital id which is created are static which is less secure compared to the dynamic digital id which are randomly given and keeps on changing after regular intervals which has been deployed by Singapore Trace Together app.[16]

Thus, given the nature of these apps and data that is been mined by the apps in the user phone and devices and the mandatory use of such apps have posed not only legal, ethical and technological challenges but also has raised privacy concerns in the country like India and others who don't have strict data protection law nor privacy laws or health data privacy law and their defined uses and interferences.

## IV. ISSUES WITH THE DIGITAL CONTACT TRACING APPS

The use of digital contact tracing has raised concerns about its use, purpose, privacy concerns, data management and legal framework for such apps. Issues primarily have been raised due to the existing mistrust of the people in the

---

[12] GAO@100, Science & Tech Spotlight: Contact Tracing Apps ( September 24, 2021) <https://www.gao.gov/products/gao-20-666sp>.

[13] Ministry of Electronics & Information Technology Electronics Niketan, New Delhi , (September 27, 2021) <https://static.mygov.in/rest/s3fs-public/mygov_159050700051307401.pdf>.

[14] Exposure Notifications: Using Technology to Help Public Health Authorities Fight COVID-19' ( last visited 24 June 2020) <https://www.google.com/covid19/exposurenotifications/>.

[15] AarogyaSetu, Privacy Policy, (last visited October 12, 2021) <https://web.swaraksha.gov.in/ncv19/privacy/>.

[16] Ankit Kumar, "How Aarogya Setu Works, and How it Compares to Contact-tracing Apps in Other Countries", *India Today* ( May 6 , 2020, 20.49 pm), <https://www.indiatoday.in/technology/features/story/how-aarogya-setu-works-and-how-it-compares-to-contact-tracing-apps-in-other-countries-1674966-2020-05-06>.

public authorities and various intermediaries involved in making such apps and collection and use of data by such entities. Misinformation about legal, ethical and technological knowledge also have led to the polarisation of such debate. However, such a pandemic requires some strict and rapid measures by the authorities for the betterment of humanity but such measures should be based on reasoned and informed decisions.

## V. PRIVACY AND DATA COLLECTION CONCERNS

The digital contact tracing app has once again raised privacy debates over the privacy policies of the app as well as the country and also the collection and use of data by these apps. There are three different aspects of privacy protection, one privacy policy given by the app, every app has their own privacy and data collection and uses rules which sometime are mandatory like recent new Whatsapp data sharing rule, Arogya Setu privacy policy from which you cannot derogate since they are not discretionary one has to comply if he wants to use the app.[17] Second aspect of privacy is national privacy and data protection laws. Many countries have a defined privacy law Like Europe GDPR which makes mandatory for all applications and their privacy policy to comply with such law but many developing countries like India itself lack such data protection law, which is still in the raw stages of development and privacy has been only recently recognised as a fundamental right itself. Thus, making such a data collection app as Arogya Setu in India mandatory is a huge violation of individual human rights. Third aspect of privacy is control over privacy given to the user by these apps which gives users the authority to manage their own data.[18] Data collection, storage and its examination can be shared which is why such data is always at risk of abuse. Certain important data is mined by these apps for the proper functioning of the app like location history, contact, name, health information and some even use social media information for tracing an individual. This is a typical concern with most of the apps like China's 'Contact-Detector' uses health and travel data of an individual which is analysed and given risk colours, essentially denying them essential services.[19] According to the data collected by Digital Rights Tracker around 19 apps tallying of 4 million downloads did not have privacy policy of their own[20] like in the case of Indian Arogya setu app also initially the government did not specify its privacy policy. It was later on when hue and cry was made by the community of people, then the privacy policy was laid down and it was

---

[17] *Supra* note 8 at 9,10.

[18] Michele Loi et al., Ethical Framework for Human-Centric Public Health Digital Surveillance (Public Health Digital Surveillance) (June 19, 2017) <https://docs.google.com/document/d/19F_hXIIPvDKCk8JTfxNXOuex0r_GpmPEUuoSUMEj-zY/edit?uspl/4embed_ facebook> accessed 2 July 2020.

[19] Raymond Zhong, "China's Virus Apps May Outlast the Outbreak, Stirring Privacy Fears", *The New York Times* (May 26, 2020) <https://www.nytimes.com/2020/05/26/technology/china-coronavirus-surveillance.html>.

[20] *Supra* note 10.

substantially updated overtime.[21] Secondly the data which is collected by these apps is often at risk due to the lack of proper guideline of its use and accountability also due the luddite of people who doesn't know the proper functioning of such apps like once data is collected how it is to be stored and who can access it, how long it will stored and what will happen once the pandemic is over, often the entities making such apps does not take the accountability on the leak of such informational data.[22] Thirdly, lack of the technique of collecting anonymized data or maintaining anonymisation of collected data is very difficult and financially huge due to which many times public authorities often give promises of keeping data as anonymised but these are just pseudo-anonymity.[23] A study done in 2013 which collected location data of an individual which was supposed to be anonymised found out that it was so explicit to singular propensities, over a million of people can be traced from just three or four given the points based on their regular habit.[24] Due to these concerns several other apps have been launched which track the violations and misuse of cyber rights on an individual by the implementation of these apps like pandemic big brother[25] and digital rights tracker.[26] Such app design and other protective and policy measures have to been taken by the government authorities to build a trust in the public at large, not only measure but the government and other intermediaries involved in such process also needs to be accountable for any misuse of such data because such health data can be very useful on the large scale for health research and also for other such upcoming pandemic. If applied appropriately such data collection and surveillance apps can prove to be effective.[27]

Battling against the pandemic through computerized contact surveillance technology might require impermanent reductions of privacy and individual's data. Since it possibly raises restrictions to individual privacy and data, people ought to be informed to complete these decisions themselves to fabricate trust for reception of these technologies.

---

[21] Meryl Sebastian "Aarogya Setu's 6 Major Privacy Issues Explained", HuffPost (May 13, 2020, 5.17 a.m.) <https://www.huffpost.com/archive/in/entry/aarogya-setu-app-privacy-issues_in_5eb26c9fc5b66d3bfcddd82f>.

[22] Andres Calderon et al., "Privacy, Personal Data Protection, and Freedom of Expression under Quarantine? The Peruvian Experience", 11, No., International Data Privacy Law, 2021, 48 (2021).

[23] Laura Bradford et al., "COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR, and Data Protection Regimes", 7 J.L. & Biosciences 1 (2020).

[24] Yves Alexandre de Montjoye et al., "Unique in the Crowd: The Privacy Bounds of Human Mobility", 3 Scientific Reports, 1376 (2013).

[25] Pandemic Big Brother <https://pandemicbigbrother.online/en/> ( last visited September 24, 2021).

[26] *Supra* note 10.

[27] European Data Protection Board, 04/2020, Guidelines on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak, (21 April 2020). <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf>.

## VI. LEGAL AND ETHICAL ISSUES

Information that is being mined by these apps is considered as personal data of a living human being and data related to covid-19 is specially comes under special category of personal data i.e. health, under many regimes of law of various nations.[28] In the era of modern technologies and the ongoing pandemic, it requires huge data collection for the purpose of medicinal research and also for disease prevention. Thus, opening of resources and wide access to these apps to collect health data which is highly protected and sensitive information and sharing of the data with the national and international health community is essential for the development of modern medical treatment and scientific enquiries. For the collection of sensitive health data of an individual one has to compromise with his or her data privacy but that compromise should be based on rational situations and purposes. Many researchers scale out these measures that such compromises with the data and privacy of an individual should have compliance with the fundamental rights of those individuals and data protection laws of the nation.[29]

However, given the situation and urgency of the pandemic which many countries are still trying to cope up with and the lack of medicinal emergency which required rapid collection of data and making and deployment of proper medicines, and technology which has added to the situation and ultimately ousted the privacy. Many countries contact tracing applications have been backed and underpinned by law regimes which makes them responsible to the public like Europe GDPR, South African Protection of Personal Information act of 2013 ( POPIA)[30] and UK data Protection Act[31] etc. but many countries are still in the raw stages of drafting such bills Like India, Pakistan, and Thailand. Few countries even have such law but their law regimes may have become redundant over the technological advancement happening every day.[32]

India, is still in the early stage of enacting a proper data protection bill which has been drafted but lacks certain considerations which is being debated over by the parliament.[33] In India online collection of data is still managed and controlled by Information and Technology Act, 2000 and IT rules[34] but

---

[28] *Supra* note 23 at 3, 4.

[29] Nóra Ni Loideai, Regulating Health Research and Respecting Data Protection: A Global Dialogue,10 International Data Privacy Law, 2020, 115 (2020).

[30] Protection of Personal Information Act, 2019, <https://popia.co.za>.

[31] Data Protection Act 2018, <https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf>.

[32] SachaAlanoca et al., "Digital Contact Tracing Against COVID-19: A Governance Framework to Build Trust", 11 International Data Privacy Law, 2021, 11(2021).

[33] The Personal Data Protection Bill, 2019, <https://prsindia.org/billtrack/the-personal-data-protection-bill-2019>.

[34] Vijay Pal Dalmia, Data Protection Laws in India - Everything You must Know, Mondaq (December 13, 2017) <https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india--everything-you-must-know>.

current information and technology act is somewhat not compatible with the present technology of contact tracing application and the data protection of an individual particularly health. Section 69 of present IT Act[35] provides certain exceptions when the government and any entity with the written order of the government in the interest of sovereignty or integrity of India, for defence and security of the State, friendly relations with foreign States and for preventing incitement to any offence, can monitor , decrypt any information stored in computer resources.[36] The act also provides penalties in case of any violation of confidentiality and privacy of information under section 72[37] but the act does not define what is personal data of an individual nor gives protection to other types of data of an individual including health , location etc. as have been covered in GDPR, POPIA, HIPAA and others. Indian Data Protection Bill also provides for the data localization which means that information or information related to Indian citizen will be stored and processed in India only and no company and authority will be allowed to carry data outside India nor that be used outside the country i.e. a mirror image or copy of data is kept in the country and data processing entities will be barred from sharing and transferring critical personal data, however the bill lacks the definition of what amount to critical personal data.[38] Data localisation technology has many positive aspects, for example local storing of data will help legal enforcement agencies to use the information for the benefits of national interest both strategically, medically and economically. Secondly, preservation of such data can also empower the nation and its ability to tax internet giants and also favouring national companies infrastructurally and giving more employment which will give a boost to the start-up economy and AI regime.[39] Thirdly such data localization can in some way protect individual privacy as by making compliance with Indian law where people will have regional and local remedies against such companies.[40]

One of the most important ethical issues that arose in many countries was the government agencies did not provide proper guidelines for the data usages of these apps and neither the ways in which it is protected. Many apps like Argentina Cuidar App and Brazil IBGE circular made mandatory collection of such data which could be later shared with other entities for research in the medical field and developing statistical data for further pandemic which was criticized by civil society members.[41]

---

35 Information Technology Act , 2000.

36 *Ibid.*

37 *Ibid.*

38 *Supra* note 33

39 Rishab Bailey, The Issues Around Data Localisation, *The Hindu* (Feb. 25 , 2020) <https://www.thehindu.com/opinion/op-ed/the-issues-around-data-localisation/article30906488.ece>.

40 *Ibid.*

41 Tais Fernanda Blauth et al., "Data-Driven Measures to Mitigate the Impact of COVID-19 in South America: How do Regional Programmes Compare to Best Practice?",11 International Data Privacy Law, 2021, 25 (2021).

## VII. DIGITAL INCOMPATIBILITY CONCERNS

When we discuss about digital measures and means to be adapted for controlling and surveilling any problems related to health or others, one cannot avoid to afford a view of the critical portion of the population that does not possess such digital means or those who have means but lacks digital knowledge to use such means. As seen in many nations like Germany, which has 99% literacy rate[42] but still such apps have created an economic digital divide between marginalised, deprived and wealthy people giving provocation to the problems.

Socio- economic capacity and digital access of the population of India cannot be overlooked when making such apps. One has to consider the viability and compatibility of such apps and technology with the prevailing population. Firstly most of the people do not have proper digital infrastructure or means to get such smartphones and laptops which has highlighted and moreover created the digital divide in the country where one lacked proper means to access proper information and continuance of their routine activities like proper education.[43] Secondly, even if people have such infrastructure, they still lack the digital awareness for using such technology and updating the apps from time to time. In India there stood 749 million mobile user which had access to internet from their phone[44] but according to the definition of digital literacy only 38% of Households in India are digitally literate[45] which has highlighted the gaps in the education system with the modern and rapid changing world system. Thirdly, many apps require the latest smartphone technological operating system which may not be available with many people.[46] In the European Nations, out of a total 85% of people using the internet via mobile phones only 58% of them had basic digital skills.[47] Fourthly people using such apps do not know about the functionalities of these apps and how to self-access them routinely which led to incorrect collection of data Argentina Cuidar App had 5.5 million self-evaluated tests but only 5 million people had downloaded the app which shows discrepancy in the app itself.[48] Thus many countries still lack 'cultura digital' which is one of the most important causes of the failure of such technology.

---

[42] Macrotrends, <https://www.macrotrends.net/countries/DEU/germany/literacy-rate>.

[43] *Supra* note 41.

[44] STATISTA, <https://www.statista.com/statistics/558610/number-of-mobile-internet-user-in-india/> (last visited October 5, 2021).

[45] Venugopal Mothkoor, "The digital dream: Upskilling India for the future", Ideasforindia (March 23,2021), <https://www.ideasforindia.in/topics/governance/the-digital-dream-upskilling-india-for-the-future.html>.

[46] *Supra* note 41.

[47] European Commission, Digital Economy and Society Index Report (July 11, 2020), <https://ec.europa.eu/digital-single-market/en/human-capital>.

[48] *Supra* note 41.

## VIII. COMBINATION OF MEASURES THAT CAN BE ADOPTED FOR THE PROTECTION AND CONTROL OF RISK INVOLVED IN DATA COLLECTION AND USES

Digital Surveillance Technology has been a core tool for the protection, monitoring, controlling, tracing, notifying and assessment of the spread Covid19 pandemic. The pandemic and public health surveillance requires the working of different agencies both governmental, legal and health and technology development sectors together to bring about more effective and interdisciplinary approaches to govern such pandemic and make the technology more accessible and easy to use, understood by the community for which it has been adopted. Legal agencies and governments need to work on the proper mechanism to bring more accountability by these entities who are collecting and disseminating personal data of the community.[49] Of particular importance is the consideration of epidemiological considerations in the development and implementation of digital tools, including usability on mobile devices, interoperability, regulation of literacy and compatibility with disabilities, as well as incentives for their adoption.[50] Moreover it will be both judicious and attainable for every nation to make such digital surveillance tools more transparent and adaptable not only for the present Covid19 pandemic but for other outbreaks of such infectious diseases.

Public health surveillance is not a new phenomenon, and it has been used by different nations all over the world to control the outbreak of various diseases such plague, smallpox, Ebola etc. by various nations in the past.[51] The only difference that lies in the data collection measures today from the past is deployment and exploitation of digital technology. Public health surveillance in India is considered as a different activity and not related to health care service delivery. India has traditionally focused on surveillance for communicable and infectious diseases like Aids, Polio etc. But digital contact tracing is employed for the first time in India, and it is the first digital surveillance system in India. However, steps are being taken for the implicating and forming a more compliance based digital surveillance in the country by Niti Aayog and other health providers and a health id card also is in the process of being made.[52] Enhancing public health surveillance is an important public health function which includes detection of diseases and early warning signs of impending outbreaks both nationally and internationally. Many new measures and technology have come up that can be used as an alternative or by making the present technology and app used in surveillance more robust.

---

[49] DivyaRamjee et al., "COVID-19 and Digital Contact Tracing: Regulating the Future of Public Health Surveillance", 2021 Cardozo L. Rev. De-novo, 101 (2021).

[50] *Ibid.*

[51] Bernard C.K. Choi, "The Past, Present, and Future of Public Health Surveillance", (August 5, 2012) <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3820481/>.

[52] <https://www.niti.gov.in/sites/default/files/2020-12/PHS_13_dec_web.pdf>.

Few alternative measures have been developed in recent times which can be adopted to combat these issues areas follows-

## A. Decentralized Data Contact Tracing Apps

Decentralized data contact tracing app uses GAEN API which is considered as safer technology if compared to Centralized location and Bluetooth based apps. Many nations like Belgium and Switzerland are using decentralized Bluetooth based apps which prevents data storage and data sharing on some third platform. User data is stored in their own devices which is shared with other users only when someone comes in contact near it, thus preventing other governmental or government empowered entities from collecting proximity data of the user, which leads to reduction of user privacy data risk.[53] Recent trends have shown that privacy advocates have more inclination towards developing and using more widely accepted protocols like PACT, DP-3T88[54], NFC and using decentralised Bluetooth apps for surveillance because they are less endangered to hacking and leaks.[55]

The impossibility of having a unified solution should not hamper the development of a national network that uses specialists from relevant sectors to make a stabilized contact tracing initiative. This requires that health authorities and developers of digital surveillance tools consider: (1) regulating standards for universal usability and accessibility, and incentives to encourage adoption and engagement with applications[56]; (2) apps that are feasible for people with older mobile devices other than smartphones; (3) state issues related to biometric privacy regulations, application interoperability across state borders, and application usage enforcement in different jurisdictions; and (4) privacy and security laws and decisions related to medical information and mobile data collection.[57]

## B. Consent to Opt-In/Opt-Out

Government and other authorities should require an explicit consent of an individual prior to collecting and disclosure of such health data with another

---

[53] Marcel Salathe et al., "Early Evidence of Effectiveness of Digital Contact Tracing for SARS-CoV-2 in Switzerland", Swiss Med. Wkly. (December 16, 2020), <https://smw.ch/article/doi/smw.2020.20457>.

[54] Justin Chan et al., "Pact: Privacy Sensitive Protocols And Mechanisms For Mobile Contact Tracing", 13 (2020), <https://arxiv.org/pdf/2004.03544.pdf>.

[55] Tim Starks, "Early Covid-19 Tracking Apps Easy Prey for Hackers and it Might Get Worse Before it Gets Better", Politico (July 6, 2021, 7.00 p.m.), <https://www.politico.com/news/2020/07/06/coronavirus-tracking-app-hacking-348601>.

[56] *Supra* note 49

[57] Benjamin Boudreaux et al., "Strengthening Privacy Protections In Covid-19 Mobile Phone Enhanced Surveillance Program"s (2020), <https://www.rand.org/content/dam/rand/pubs/research_briefs/RBA300/RBA365-1/RAND_RBA365-1.pdf>.

device or network. Consent includes two meanings: firstly, in the field of research consent is an ethical principle that one should take prior and informed consent from a participant before taking samples and surveys. Secondly consent has another meaning which means consent as a legal rule before processing personal data of an individual, many countries have different laws relating to consent in processing of data. Health Data in many jurisdictions is considered as personal data but even though many nations that have law which requires prior consent for processing personal data makes an exception in the law for consent with respect to health data due to public benefits.[58] GDPR and HIPAA also makes an exception for using personal data of user relating to health no prior consent is needed but EU nations have laws that makes consent for health data mandatory[59]. California's (CCPA) California's Consumer Privacy Act[60] and Biometric Information Privacy Act (BIPA)[61] Illinois have created a more robust tory framework system for collection, using and sharing of biometric data and they have also provided for the accountability of entities by giving right of action to the individuals. However, collection of data for public health emergencies and public health surveillance require special consideration for which government should be able to collect data for public health research to make public health better.

## C. Incentivisation, Adaptation and Development of Technology

Mere making of apps and development of technology is not enough to fight such pandemic. To do research-based study by these apps one needs to see the socio-economic and literacy means of a country. Before laying down such technology for surveillance[62], the government should see whether such technology will be used by the population for which one needs to satisfy the various doubts of a user relating purposes of such data collection and its uses, mitigation and privacy norms. Data Portability can also be used for developing trust in the public which gives powers to users to transfer their user data to any entity who offers more reliable services.[63] Doubts and trust issues in the minds of the people related to them have led to the failure of the apps in many nations, thus the government needs to adopt a more user-friendly technology accessible to all and give incentives for using such means.[64]

---

58 Edward S. Dove et al., Should Consent for Data Processing be Privileged in Health Research? A Comparative Legal Analysis, 10(2020), International Data Privacy Law, 118 (2020).

59 *Ibid.*

60 Biometric Information Privacy Act (BIPA), 2008 Ill. Laws 994 (codified at740 ILL. Comp. Stat. 14/1-99 (2020)).

61 California Consumer Privacy Act of 2018 (CCPA), 2018 Cal. Stat. Ch. 55, §3 [codified as amended at Cal. Civ. Code §§ 1798.100-99 (West 2020)].

62 *Supra* note 49.

63 Giuseppe Colangelo et al., "Data Accumulation and the Privacy-Antitrust Interface, Insights From the Facebook Case for the EU and the U.S.", 8 (2018), International Data Privacy Law, 2018.

64 Elad D. Gil, "Digital Contact Tracing Has Failed: Can It Be Fixed with Better Legal Design?" 25 Va. J.L. & Tech. 1 (2021).

## IX. CONCLUSION

The coronavirus pandemic has taken a severe resilience test of all the nations around the world. To control such fast spreading of viruses called for a public health emergency for the search of mitigation strategies which ultimately led to the contact tracing apps via database sharing technology. Countries faced similar challenges such as privacy issues, human rights, technological issues, low usage rates due to trust issues in technology, and purposes of data collection by the government and apps. Issues with respect to technology, legal, ethical and sociological issues have been addressed and analyzed in this article with a comparative approach with other nations' apps and India. Therefore, this article proposes a more transparent structure of sharing data about personal health of an individual while at the same time protecting his or her privacy by using various alternative technologies such as anonymization. If trust cannot be assured, then low adaptability rates of apps will prevail which will hamper all together the purpose of such apps. Trust issues can be assessed in a more guided manner with laying down proper rules and regulation to make compliance of data collecting authorities to laws made by the government in case of misuse, data leaks of such personal data. Data collected through these apps should be only used for Covid-19 and not for another further research like in Brazil. Private health data collection of an individual is crucial for controlling and building a resilient system of public health by the nations and to control and do research for further such pandemic. Further, not all problems can be solved just by making an app nation should adopt a wider approach to combat such a public health emergency which is accessible to all levels of population.