PRIVACY AND CONFIDENTIALITY OUTLOOK ON CONTACT TRACING APPLICATIONS

Jumanah Kader, SASTRA Deemed University

ABSTRACT

Contact tracing applications are tracing applications to curb the spread of the virus. In due course of tracing, these applications violate several privacy concerns of the individuals. Besides, when Governments use the collected data for a purpose other than the intended one (which is curbing the transmission of the virus), it amounts to a breach of the principle of confidentiality. Thereby, it is safe to say that the effective use of contact tracing applications requires proper balancing to ensure right to privacy is protected at all cost. In these pages the author has made a small attempt to right the ship by offering a primer on contract tracing apps and right to privacy. The constant tug-of-war between the duty of the government to protect the individuals and the right to privacy of an individual is also dredged up in this paper. Lastly, the authors conclude by reiterating the positive content of privacy as attracted by the decision of the landmark case in *Justice K. S. Puttaswamy (Retd.) and Anr. vs Union of India and Ors*[1].

[1] *K.S. Puttaswamy and Anr. v. Union of India*, (2017) 10 SCC 1.

I. INTRODUCTION

The power of sensation is extramundane in this avant-garde era. Hence, no wonder why we have the power to bend and mend matters with technology. The said weapon has become a leviathan to meet the ends of a global crisis that we are facing today under an application that emphasizes the idea, "*prevention is better than cure.*" The invention of "*contact tracing apps*" has become the northern star in aiding the covid warriors. If a solution to any problem is easily derivable then, it is not a solution. In that light, although the contact tracing apps offer an incredible solution to get away with the virus spread, the issue of surveillance and breach of privacy taints the incredibility.

II. RIGHT TO PRIVACY THROUGH THE LENS OF HUMAN RIGHTS AND THE INDIAN CONSTITUTION

Right to privacy, in the international setup, is guaranteed under Articles 12[2] and 17[3] of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights respectively. It also occupies an integral place in various other international treaties and conventions. These rights enumerate the consequential aspects of an individual's privacy. It is been said that privacy is one of the most undefinable rights[4], although there is a bounteous explanation for the said term. In that light, we reiterate the observation of two authors, *"in one sense, all human rights are aspects of the right to privacy*."[5] This international preview of right to privacy is painted similarly in the Indian Constitution.

A. Right to privacy under right to life and liberty

Right to privacy, in India, became an explicit part of fundamental rights in the year 2017[6]. Hon'ble Justice Abhay Manohar Sapre beautifully explained the existence of privacy under Article 21, and here we quote:

"...emanating from expression personal liberty" under Article 21 Right to privacy is inbuilt in those expressions and flows from each of them and in juxtaposition Right to privacy is part of

[2] UDHR § 12 (1948)
[3] UDHR § 17 (1948)
[4] Micheal James, *Privacy and Human rights: an international and comparative study, with special reference to developments in informational technology*, January 2020, available at (https://catalogue.nla.gov.au/Record/2133144) (Last visited on 7th December, 2023).
[5] Louis Henkin, *The international Bill of Rights: the covenant on civil and political rights*, January 2020, available at (https://catalogue.nla.gov.au/Record/1578645) (Last visited on 7th December, 2023).
[6] Supra, at 1.

fundamental right of citizen guaranteed under Part III of Constitution, not absolute right but subjected to reasonable restrictions…"[7]

Therefore, right to privacy is also guaranteed under the Indian Constitution but is subjected to certain "*reasonable exceptions."* These exceptions determine the length and breadth of the freedom so guaranteed. The Constitution protects the right of an individual from being infringed and it has facilitated other statutes for safeguarding all the other colours of privacy.

B. Regulation of right to privacy via a statute - the IT Act, 2008

Right to privacy in the digital world is, to date, governed by the Information Technology Act, 2000 (as amended by the Information Technology Amendment Act, 2008) read with the Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011 (SPDI Rules). Technology is a growing giant and to match privacy's pace with it, the Personal Data Protection Bill, 2019 (Bill), is under the roof. When there is a right, there are tactical ways to admonish that right, especially in this technologically backed world. Therefore, having said about the ambit of privacy, the authors would like to navigate to the extended concept of privacy.

C. The extended concept of right to privacy

There are eight identified concepts of privacy that together build the tower of right to privacy. These include: Bodily privacy - the privacy of one's physical body; Spatial privacy - privacy of a private space; Communicational privacy - privacy in restricting the access to communication; Proprietary privacy - privacy to use property; Intellectual Privacy - privacy in rationality and the likewise; Decisional Privacy - privacy in making decisions; Associational Privacy - Privacy in acquaintances and forming associations; Behavioral Privacy - privacy in preserving oneself from unwanted intrusions; Informational privacy - privacy in preserving one's information from being disseminated and controlling the extent of access[8]. These concepts along with reasonable exceptions keep the quest of privacy unanswered.

III. REASONABLE EXCEPTIONS OR RESTRICTIONS - ANOTHER CONCEPT OF PRIVACY?

The concept of privacy gets widened and sometimes shrunken with reasonable exceptions. It is so because it differs from case to case, and that what was found to be reasonable in one case

[7] Id.
[8] University of Pennsylvania Journal of International Law, 5 Jan 2020, available at Vol. 38 Issue 2 (https://scholarship.law.upenn.edu/jil/vol38/) (Last visited on 7th December, 2023).

may not be the same in another. The test of reasonability has been underlined in Articles 14, 19, and 21 of the Indian Constitution. The basic premise of the said test postulates the following:

- The need for an existence of a law; and
- The law should not be arbitrary; and
- The infringement of the right by such law should be proportional for achieving a legitimate state aim.

The author, hereby, quote the relevant paragraph from the landmark judgement -

> *"The state must nevertheless put into place a robust regime that ensures the fulfilment of a three-fold requirement. These three requirements apply to all restraints on privacy (not just informational privacy). They emanate from the procedural and content-based mandate of Article 21."*[9]

When a law, which is alleged to violate the fundamental rights of the people, is subjected to the '*three-fold requirement'* test, if it satisfies the test then such a violation gets covered under the ambit of reasonable restrictions. If such a law does not get covered within the ambit of the test, then it is in outright violation of the fundamental rights of the people.

IV. DISTINCTION BETWEEN THE POSITIVE AND NEGATIVE OBLIGATIONS OF THE STATE

Every state has positive and negative obligations[10]. Where a state has positive obligation, it must take all measures to protect a right. It must endeavour to ensure effective enjoyment of an individual's right[11]. Per contra, by negative obligation, a state has a duty to not to act. It cannot impose laws infringing human rights. In that light, Justice Chandrachud, in the course of his judgment for the Constitution Bench in *Minerva Mills Ltd v Union of India*[12] narrated the following:

[9] Supra. at 5.
[10] *Velásquez-Rodríguez v. Honduras*, (1989) 28 ILM 291.
[11] *Neira Alegría et al. v. Peru, Merits*, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 20.
[12] *Minerva Mills Ltd. and Ors. v. Union of India (UOI) and Ors*, AIR 1980 SC 1789.

"Both Parts III and IV of the Constitution had emerged as inseparably inter-twined, without a distinction between the negative and positive obligations of the state."[13]

It is consequential to understand the difference between the positive, and the negative obligations of the state to process the rationality in the interference of the state in any dispute concerning rights of the people.

A. Right to privacy and the positive obligation of the state:

The right to privacy can be both negatively and positively defined[14]. Negative definition asserts that an individual's right to privacy is protected from unwanted intrusion. Whereas, the positive definition allows the state to undertake its positive obligation. In other words, *"...as a positive freedom, it obliges the State to adopt suitable measures for protecting individual privacy."*[15]

Adding on, the bench firmly asserted that any infringement on the right to privacy can be made by a law which is "*fair, just and reasonable." From this it is evident that, right to privacy can be compromised at the cost of a law that is "fair, just and reasonable."* Besides, it must pass the strictest scrutiny test that proves the compelling claim of the state to infringe the right of an individual. Therefore, invasion of privacy is justified when it is done in a "*fair, just and reasonable"* manner by the state for fulfilling its positive obligation.

V. CONTACT TRACING APPLICATIONS – ITS WORKING AND IMPACT

Just 10 years back, we were not dwelling in the heights of technology. The pandemic then was also as disastrous as it is now but today, we have an option that could considerably reduce the spread of the virus - contact tracing apps. Now, having understood the breadth and length of right to privacy in the national as well as in the international regime, it is imminent to take a look at the working and impact of contact tracing apps. It is so because only when we understand the functioning of these apps, we will understand its effect on privacy rights.

A. The working of contact tracing apps

The contact tracing technology prevents the further spread of virus by indicating the presence of an infected individual. For the said purpose, it records the name, mobile number, age, gender,

[13] Supra, at 1.
[14] Id.
[15] Id.

profession, travel history, etc. of the users of the app[16]. This recording and storing of information are subject to the criticism that it violates the privacy of an individual. It is said that from the onset of the pandemic, over 45 contact tracing apps in over 25 countries were developed. One common aspect in the working of contact tracing apps is that it stores information and that is its drawback, too.

At this juncture, the author puts that in a contact tracing application, a reasonable man with reasonable prudence would know that contact tracing app will collect data for identifying a person and their exposure to an infected person because without such information there would be no means for assessing the transmission of the virus. Given the purpose of the app, it is not right to say that the general public had a reasonable expectation of privacy while using the contact tracing application. In arguendo, they had a reasonable expectation, it is not the one the society is prepared to recognize as reasonable. This argument is further buttressed by the fact that the data provided by the users of the app were used solely for tracing and curbing the spread of the virus. Thereby, the working of a contact tracing app in connection with reasonable expectation of privacy has been established.

B. Contact tracing app's impact on the global level

Contact tracing apps were initially launched in China and it played an extremely crucial role in arresting the spread of the virus. The trend was then followed by Hong Kong, Taiwan and Korea. These countries ensured the efficient use of the said application. Australia and Singapore are also on the list. The tracing app's flaw was tremendously witnessed in Qatar. Following that, Poland started debating the privacy issues associated with the app. Saudi Arabia, UAE, and Bahrain issued warning of jail terms for the non-users of the app.

Switzerland has launched the world's first contact tracing app built on the API platform developed by Google and Apple together. UK, Germany, Italy, Austria and Ireland are also following the footsteps of Switzerland. In our country, we have the Aarogya Setu app - the most downloaded app in the year 2020. Countries are on a race to build an app that will arrest the spread of the virus by taking into account the privacy issue involved in it.

C. John Hopkins's report on contact tracing apps

[16] Saurav Basu, *Effective Contact Tracing For Covid-19 Using Mobile Phones: An Ethical Analysis Of The Mandatory Use Of The Aarogya Setu Application In India*, September 2020, National Library of Medicine (Cambridge University; 2020) available at (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7642501/) (Last visited on 7th December, 2023).

John Hopkins University's Berman Institute for Bioethics together with the Center for Health Security released a report on 27th May 2020 concerning contact tracing apps and covid 19. One of the primary conclusions of the report mandated that privacy should not outweigh public health goals and other values. Hereby, the effectiveness of contact tracing apps is bright as the sun. Jeffrey Kahn, the director of the Berman Institute, highlighted the importance of balance between privacy of an individual and health of the general public, and the same is quoted below:

> *"As we move forward, we must strike a balance between privacy and values like equity, choice, economic well-being, and solidarity. Too much emphasis on privacy could severely limit the ability to gather information that is critical for effective and efficient contact tracing to help beat the pandemic…"*[17]

VI. CONTACT TRACING APPLICATIONS AND RIGHT TO PRIVACY – NOT AN OXYMORON:

"In this time of COVID-19, digital technologies have an unprecedented capacity to accelerate and improve the way the world responds to infectious disease outbreaks and pandemics…" said the President of Johns Hopkins University, Ronald J[18]. Daniels in relation to contact tracing applications. Thereby, it is evident that the effectiveness of using contact tracing applications is undeniable. Thus, when there are instances of privacy violation, appropriate action must be taken by the State to prevent misuse of data and fundamental rights.

In the first instance, there should be no violation of privacy at all. In order to make that a reality, States must ensure that they have an unbreachable security system in place to protect the data of the public. Then in any instance if there is privacy breach, strict action must be taken. When such a balance between right to privacy and techno solutionism is ensured, contact tracing applications and right to privacy does not become an oxymoron. Moreover, since the contact tracing apps do not give space for reasonable expectation of privacy, in essence, there is not violation of right to privacy.

---

[17] *Johns Hopkins University*, Johns Hopkins Releases Comprehensive Report on Digital Contact Tracing to Aid COVID-19 Response, May, 2020, CISION PR Newswire, available at (https://www.prnewswire.com/news-releases/johns-hopkins-releases-comprehensive-report-on-digital-contact-tracing-to-aid-covid-19-response-301065473.html) (Last visited on 7th December, 2023).

[18] Id.

VII. CONCLUSION

Contact tracing app's fundamental function is to prevent the spread of the virus. On account of doing the same, there are possibilities for infringing the privacy protocol. Attention must be given for improving the loopholes instead of abandoning the tracing technology. The author suggests that block chain technology could be employed to secure the collected data from privacy breach. Thereby, right to privacy of the people will be balanced with the positive obligation of the State. This balancing aspect has been highlighted by the pronouncement of Justice Nariman in the *Puttuswamy case*[19], when read in conjunction with the statement of the President of Johns Hopkins University, Ronald J. Daniels[20] on the importance of contact tracing applications. Thus, for curbing the spread of the virus, contact tracing apps play a vital role and the same must be duly recognized even from the lens of privacy. One such recognition could be by employing the blockchain technology.

[19] Supra, at 1.
[20] Supra, at 18.