Guest Report: Bridging Concerns with Recommending Aarogya Setu

20 June, 2020

By **Siddharth Sonkar**

Edited and Reviewed by **Arindrajit Basu, Mira Swaminathan, Aman Nair**

The Centre for Internet and Society, India

GUEST REPORT: BRIDGING THE CONCERNS WITH RECOMMENDING AAROGYA SETU

SIDDHARTH SONKAR[1]

TABLE OF CONTENTS

[1]Siddharth Sonkar is a final year student of the National University of Juridical Sciences (NUJS), Kolkata with a sustained interest in law, technology and regulatory policy. Siddharth is graduating with the class of 2020.

ACKNOWLEDGMENTS

A big thank you to Arindrajit Basu, Aman Nair and Mira Swaminathan at the Centre for Internet & Society for a prompt and seamless editorial process and their valuable comments and suggestions; Professor Dr. Aparna Chandra, Professor Saurabh Bhattacharjee and Professor Mahesh Menon for their prompt and valuable comments and suggestions; Divij Joshi for his valuable and timely suggestions and feedback; Vasudha Passi for necessary inputs and edits towards finalising the draft; Agrim Mittal for providing the necessary technological expertise in understanding the extent to which the source code revelation results in algorithmic transparency, Professor Shouvik Kumar Guha for offering a wonderful elective course on Artificial Intelligence at NUJS, and giving us great clarity on the theory of algorithmic biases and disparate impact on vulnerable groups; Professor Agnidipto Tarafder for ending the Privacy course at NUJS with a beautiful question paper on the legality of contact tracing apps in our privacy examination; and all the faculty for being supportive and encouraging us to write and engage in critical thinking

EXECUTIVE SUMMARY

Aarogya Setu collects real-time location data of users every fifteen minutes to facilitate digital contact tracing during the Pandemic. It *inter alia* color-codes users indicating the extent of risk they pose based on their health status and predicts hotspots which are more susceptible to COVID-19.[2] Its forecasts have reportedly facilitated the identification of 650 clusters of COVID-19 hotspots and predicting 300 emerging hotspots which may have been

[2]Mint, Covid-19 contact tracing app Aarogya Setu has alerted 1.4 lakh users: Official, available at https://www.livemint.com/news/india/covid-19-contact-tracing-app-aarogya-setu-has-alerted-1-4-lakh-users-official-11589226902816.html last visited 18 June 2020.

otherwise missed.[3] In a welcome move, the source code of the application was recently made public. The initially-introduced mandate to use the application was reportedly diluted and a Protocol supplementing the privacy policy with additional safeguards was released. Despite these steps in the right direction, some key concerns continue to require alleviation through engagement. This Report seeks to constructively engage with these concerns towards making privacy safeguards governing its operability more consistent with international best practices.

First, the Report maps situations in which Aarogya Setu *in fact* remains mandatory (in Table 1) In these situations, there exists no restriction against private parties (e.g. employers, airlines, hotels, etc.) from indirectly making its use mandatory. Consequently, there is no real choice in determining the use of the application. Even where there exists a choice to opt-out (e.g. in contexts where there is only an advisory but no indirect mandate), the choice is not meaningful due to the inability to examine the potential consequences of using the application. The application remains mandatory for practical purposes since there still exists an obligation to undertake due diligence towards making sure that every employee uses the application. This part of the report explains why **it remains indirectly mandatory to use the application. This indirect mandate impedes the exercise of meaningful consent**. **This could be addressed through a notification directing that no one should be indirectly compelled to use the application.** This part also acknowledges that even where a choice to opt-out (e.g. in contexts where there is only an advisory but no indirect mandate), the choice is not meaningful due to the inability to examine the potential consequences of using the application.

Second, the report explains why the mandate to use the Application raises concerns in the first place: i.e. in the absence of transparency beyond the publication of the source code. **The open-source code** may not necessarily result in ***meaningful* algorithmic transparency** (since the processing in the models at the **Government of India server** continues to remain a black box) in respect of predictions made to determine appropriate health responses. Based on the source code per se, people are unable to verify the wherever there exists operability of the Application more meaningfully. **Algorithmic transparency enables people to make an informed decision** in using the Application by choice. The *ability* to make an informed decision is critical to the right to privacy. The right to privacy does not just mean drawing boundaries or creating limitations against any external interference. **The right also includes**

[3]Rhythma Kaul, Aarogya Setu gave forecasts regarding 650 Covid-19 clusters, 10-05-2020, available at last visited https://www.hindustantimes.com/india-news/aarogya-setu-alerted-about-650-clusters/story-1kvGonSkLz77dwH3zMYOQI.html last visited 14 June, 2020 ("Using syndromic mapping and trace history of Covid-19 positive people combined with their movement patterns and exposure of different regions to Covid-19, the Aarogya Setu team has forecasted more than 650 hotspots across the country at sub-post office level, in addition to more than 300+ emerging hotspots which could have been missed otherwise").

the public's right to know how an algorithm affects their lives. Given the centrality of transparency in the ability of the user to exercise their privacy better, beyond releasing the source code of Aarogya Setu, publicizing information about *how* predictions are made is important. **Here, the report acknowledges the limitations of transparency in that it can only facilitate identification of privacy harms and not really solve them by itself.** Yet, it goes ahead and re-emphasises the inter-relationship of transparency and privacy, highlighting how it became a basis recently in striking down a government-used algorithm, which indicates incentive to increase transparency.

Third, the report reviews whether based on the already-available information from the combined reading of the privacy policy and the protocol, the operability of the application seems consistent with best international practices in protecting user privacy. After discussing the desirable standard and intensity of judicial review, the Report structurally applies the proportionality test to identify necessary modifications to the current framework to bridge existing concerns:

1. The **'legality'** prong may be satisfied by a combined reading of the NDMA and the specificity in the delegated legislation, as has been done in the past particularly in the context of location-based surveillance. However, it is suggested (in the recommendations section) that a statutory legislation comprehensively governing the operability of the Application is introduced to ensure predictability and permanency in the framework governing the operability of the Application as done internationally. Moreover, determining appropriate health responses to the Pandemic is indeed a **legitimate interest** that is sought to be achieved through the application
2. Given the limitations of traditional methods of contact tracing, digital contact tracing could perhaps be a **suitable** method of ascertaining appropriate health responses to the Pandemic subject to a comprehensive review of evidence on a regular basis to evaluate verifiably its effectiveness. Since the use of the application seems likely in the long run, its efficacy needs to be backed by concrete evidence which corroborates its accuracy and effectiveness such as statistical data on false positives and negatives that result from the application
3. A careful reading of the combined reading of the Aarogya Satu privacy policy and the Protocol with Fair Information Protection Principles ('FIPP') indicates some inconsistencies with **international best practices**. The extent of inconsistency with best practices may not be considered the least restrictive and therefore **necessary** form in which digital contact tracing can be conducted in India
4. Since the inconsistencies seem relatively more restrictive than necessary to facilitate digital contact tracing in India, a balancing of privacy and public health could result in the conclusion that the application is not '**proportionate**' to the potential privacy harms that can result from using the application. While conducting the **balancing exercise,** privacy and public health should be viewed as **complementary, not**

competing interests. This conception would encourage courts to consider privacy concerns with sufficient extent of **intensity**[4]

Based on this analysis, the report concludes that digital contact tracing provided the following conditions (detailed in the 'Recommendations' section) are conjunctively satisfied:

1. Digital contact tracing should supplement (e.g. be in addition to) and not supplant (i.e. replace) traditional methods of contact tracing entirely, particularly for vulnerable groups (e.g. interviews where vulnerable groups, particularly marginalized women do not have access to mobile phones);
2. A statutory law should be introduced which strictly and comprehensively governs the scope of the application,
3. the suitability of the application (with meaningful algorithmic transparency) should be corroborated by reliable and relevant statistical evidence (e.g. with the help of closer scrutiny of the *basis* of predictive outcomes) and
4. The privacy compromises using the application should be intrusive to the minimum extent possible. This could be done by further adding robust safeguards through stronger restrictions on sharing the collected data.

Keywords: Aarogya Setu, Constitutionality, Digital Contact Tracing, Location Data, Personal Data Protection Bill, 2019, Exemptions, Personal Data, Sensitive Personal Data, Mosaic Theory, Surveillance, Privacy, Governing Law, Necessity, Intensity of Review, disparate Impact, Proportionality

[4]Paul Craig, 'Proportionality and Constitutional Review' (2020) 3(2) U of OxHRHJ 87 ("if a court is minded to engage in intensive substantive proportionality review it will be more minded to demand more evidence to substantiate the contested decision. By the same token, the more evidence that is seen by the court, the greater the likelihood that it will feel that it has the information from which to make an informed decision on the substance of the case").

"*When choosing between alternatives, we should ask ourselves not only how to overcome the immediate threat, but also what kind of world we will inhabit once the storm passes. Yes, the storm will pass, humankind will survive, most of us will still be alive — but we will inhabit a different world*." -Yuval Harari, The World After Coronavirus, Financial Times (20 March 2020).

INTRODUCTION

On 1st May 2020, via a Government Order ('**G.O**') under the National Disaster Management Act, 2005 ('**NDMA**') it became mandatory for employees to use Aarogya Setu ('the application'), for digital contact tracing.[5] By a subsequent Order dated 18th May 2020, the mandate was modified to suggest employers to, on "best effort basis" ensure that all employees install Aarogya Setu and regularly update their health status on the application.[6] In Massachusetts' Institute of Technology's (MIT) recent review of the application's privacy safeguards, the application fell short of scoring significantly well as compared to other contact tracing apps.[7]

The application's predictions govern access to critically important aspects of our lives: employment, flights, trains, public parks,[8] and malls[9]. The mandate to use the application received criticism for reorienting employment decisions relating to gig workers by closely monitoring their health to escape health insurance obligations towards these workers.[10] At present, data collected from the application according to the Protocol could be shared with not just research universities but research *institutions* as well. However, the Protocol does not define 'research institution' or clarify what it excludes (for instance, research units of or controlled by insurance companies or big pharmaceutical companies). Travel history mapped by Aarogya Setu can impact how much we pay as insurance premiums. The possibility of such sharing of data could significantly affect the availability of health insurance to a large

[5]Government Order No. 40-3/2020-DM-I(A), Government of India, Ministry of Home Affairs, available at https://www.india.gov.in/sites/upload_files/npi/files/MHA_%20new_guidelines.pdf last visited 27 May, 2020.

[6]Lockdown 4.0 Guidelines, available at https://pmmodiyojana.in/lockdown-2-0-guidelines/ last visited 6 June, 2020.

[7]What Purpose Does Aarogya Setu Serve Now?, Bloomberg Quint, available at https://www.bloombergquint.com/opinion/what-purpose-does-aarogya-setu-serve-now last visited 18 June, 2020.

[8]Ananya Tiwari, Abhinav Rajput, Mandatory Masks, Aarogya Setu App as Parks Open Partially to the Delhi Public, Indian Express (23 May, 2020) available at https://indianexpress.com/article/cities/delhi/new-delhi-mandatory-masks-aarogya-setu-as-parks-open-partially-to-the-public-6423259/, last visited 18 May, 2020.

[9]The New Indian Express, Aarogya Setu Mandatory for all Mall-Goers in Hyderabad, https://www.newindianexpress.com/states/telangana/2020/jun/08/aarogya-setu-mandatory-for-mall-goers-in-hyderabad-2153667.html last visited 18 June, 2020.

[10]The New Indian Express, App-based workers worry over misuse of Aarogya Setu by employers (4-06-2020)
https://www.newindianexpress.com/states/telangana/2020/jun/04/app-based-workers-worry-over-misuse-of-aarogya-setu-by-employers-2152009.html last visited 8 June, 2020.

number of people,[11] particularly the most vulnerable groups. This is because the health data of gig workers compulsorily required to use Aarogya Setu can be used to **alter the cost of premium charged** by **insurance companies**.[12] This could potentially make **health insurance more unaffordable** and consequently **inaccessible, excluding** the **most vulnerable groups** of people who need coverage the most.[13]

In a welcome move, on 27th May, via a Press Note released by the Press Information Bureau (PIB), the application was reportedly made open source in response to the criticism of the absence of algorithmic transparency in its operability.[14] This makes it possible for researchers and developers to access and inspect, and scrutinize the contents of the source code, which in turn can facilitate the identification of bugs or security-related vulnerabilities. The Government has, in another positive step, simultaneously launched a 'Bug Bounty Programme' to test the extent to which Aarogya Setu is secure.[15]

To briefly describe its roadmap, this report is divided broadly into three parts:

This report is divided into three parts broadly. First, the report maps situations in which Aarogya Setu *in fact* remains mandatory (in Table 1) In these situations, there exists no restriction against private parties (e.g. employers, airlines, etc.) preventing them from indirectly making its use mandatory. Consequently, there is no real choice exercised in determining whether to use the Application. Even where there exists a choice to opt-out (e.g. in contexts where there is only an advisory but no indirect mandate), the choice is not meaningful due to the inability to examine the potential consequences of using the application. Second, the report explains the critical importance of transparency in the people's ability to exercise their choice in using the Application more meaningfully. Transparency enables people to exercise their choices better since the consequences of these choices could have (inadvertently) disparate consequences. In the context of Aarogya Setu, releasing the server code in realizing the desirable extent of transparency and therefore addressing this particular privacy concern. Third, the report conducts a detailed

---

[11]Sohini Mitter, Aarogya Setu crosses 30M downloads on JioPhone in less than a month, YourStory (9-06-2020), available at https://yourstory.com/2020/06/aarogya-setu-crossed-30-million-downloads-jiophone-reliance, last visited 12 June, 2020.

[12]The New Indian Express, App-based workers worry over misuse of Aarogya Setu by employers, https://www.newindianexpress.com/states/telangana/2020/jun/04/app-based-workers-worry-over-misuse-of-aarogya-setu-by-employers-2152009.html last visited 8 June, 2020.

[13] *Id.*

[14]Press Information Bureau, Aarogya Setu is Now Open Source, available at last visited (27-05-2020). https://pib.gov.in/PressReleasePage.aspx?PRID=1626979, last visited 27 May, 2020; see also Indian Express, Aarogya Setu becomes open source: What does it mean?, available at https://indianexpress.com/article/technology/aarogya-setu-android-open-source-what-does-it-mean-6428458/, last visited (27-05-2020).

[15] *Id.*

review of the operability of Aarogya Setu to examine how it could be improved to ensure it is proportionate to privacy concerns during the Pandemic.

THE MANDATE TO USE AAROGYA SETU REMAINS UBIQUITOUS

Before outlining concerns regarding the governing framework (code, privacy policy and protocol) governing the operability of the Aarogya Setu, the section below indicates (i) how using the application remains mandatory and (ii) how its ubiquity affects access to essential services to a broad range of stakeholders. This section precedes the rest of the report since it underscores the significance of the report to a larger audience to begin with.

Using the application remains de facto mandatory

While the subsequent G.O is viewed as a dilution to the mandate, **employers are still required to try their best to ensure all employees download the application**.[16] It is not clear whether **failure to do so could continue to result in non-compliance with the NDMA, which in turn could invite criminal penalties**.[17] Further, the G.O dated 30 May which extended the lockdown partially till 30 June, reiterated this earlier obligation on employers: along with a new provision which enables the District Authorities to advise people to use Aarogya Setu. From the G.O, it is not clear what the penalties for non-compliance of either of these two obligations would be. The use of the word 'should' in the Order is comparable to 'may', which is often used in delegated legislation to indicate the directory nature of an obligation. A directory (e.g. an advisory or prescriptive order) unlike a mandatory order is one where no consequences flow for non-compliance.[18] To avert potential legal risks, employers would have a strong incentive to create mandates within their institutional setups requiring employees to download and use the application. As a result, the obligation on employers

[16]Stela Dey, Centre's Nudge To Employers To Have Workers Use Aarogya Setu In New Rules, NTV (30-05-2020) available at https://www.ndtv.com/india-news/mha-guidelines-on-lockdown-today-aarogya-setu-app-centres-nudge-to-employers-to-have-workers-use-aarogya-setu-in-new-rules-2237953 last visited 8 June, 2020.

[17]*Id.*

[18]*Sharif-Ud-Din vs Abdul Gani Lone*, 1980 AIR 303 ("The fact that the statute uses the word 'shall' while laying down a duty is not conclusive on the question whether it is a mandatory or directory provision. In order to find out the true character of the legislation, the Court has to ascertain the object which the provision of law in question is to subserve and its design and the context in which it is enacted. If the object of a law is to be defeated by non-compliance with it, it has to be regarded as mandatory").

arguably continues to remain de facto mandatory. It is also important to note that **employees do not have recourse against their employers if they make it mandatory to use Aarogya Setu at their establishments**.

Depending on the contextual public interest and injurious effect of failing to comply, the use of the word 'should' (or 'may') could also be understood to mean a mandatory obligation.

The pandemic arguably satisfies the public interest requirement i.e. the Government could argue that non-compliance can be detrimental to public health. That employers 'should' comply with an order sounds more pressing than suggesting that employees 'may' comply with an order: it leaves less discretion in making a value judgment regarding whether or not to comply. The modification only recognizes a practical impossibility, i.e. if installing or using the application may be impossible (e.g. smartphone inaccessibility) for employers to comply. **In all other cases, employers should put in all efforts to ensure everyone downloads the application**. Therefore, the G.O becomes a purported legal basis for employers to mandate their employees to use Aarogya Setu. If this is compared to the Aadhaar related Orders including the Aadhaar and Other Laws Amendment Ordinance, 2019, one would notice a fine difference. **The Ordinance explicitly recognized that Aadhaar verification could only be done on a "voluntary" basis** in some situations (e.g. while procuring a SIM card).[19] The Ordinance (albeit its shortcomings) **places the user at the center**, who is presumed to exercise some choice in identification. Yet, despite the Ordinance explicitly making it voluntary, the tendency to insist upon using Aadhaar for identification (such as when a customer attempts to purchase a new phone connection) has persisted.[20]

In the case of Aarogya Setu, however, if the employer makes it compulsory to use the application at a workplace, employees do not have the option to *not* download the application (since there could be consequences such as disciplinary action within the workplace).

It is an established principle that the state is under a positive obligation to protect against violation of the right by third parties[21] (such as private employers). By creating a safe harbor

[19]Section 6, Aadhaar (and Other Laws) Amendment Act, 2019 ("(3) Every Aadhaar number holder to establish his identity, may voluntarily use his Aadhaar number in physical or electronic form by way of authentication or offline verification, or in such other form as may be notified, in such manner as may be specified by regulations"); see Economic Times, Cabinet approves Aadhaar Ordinance to allow its use as ID proof for bank accounts, SIM connection, (01-03-19), available at https://economictimes.indiatimes.com/news/politics-and-nation/cabinet-approves-aadhaar-ordinance-to-allow-its-use-as-id-proof-for-bank-accounts-sim-connection/articleshow/68208198.cms, last visited 27 May, 2020.

[20]Aarogya Setu, Source Code, available at https://github.com/nic-delhi/AarogyaSetu_Android last visited 8 June, 2020.

[21]Bhandari, V., Kak, A., Parsheera, S., & Rahman, F. (2017). An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict. IndraStra Global, 11, 1-5.

(i.e. a legal basis) for employers to anchor their internal rules making Aarogya Setu mandatory, the Order in its true sense continues to remain mandatory.

In cases, however, where the mandate is diluted subsequently[22] and made into an 'advisory' or a recommendation and the private entity involved in the sector does not subsequently make it mandatory in its own capacity (e.g. employer or the airline[23]), **the earlier mandate continues to act as a strong behavioral 'nudge'**.[24] as theorised by behavioral economists, Richard Thaler and Cass Sunstein.[25] **Opting out often involves opportunity costs for the participants for which they need compelling reasons**. As pointed out in this report, people are not fully conscious (**owing to low levels of privacy literacy, a cognitive process involving thinking critically about the potential harms information sharing can/may result in**[26]) of the consequences of participating in a system that involves sharing of health or real-time location data respectively.[27] Hence, they do not realize the potential costs or harms they might be subjecting themselves to. Similar nudges in the past have preconditioned crucial

https://nbn-resolving.org/urn:nbn:de:0168-ssoar-54766-2. Gopal Sathe, A Year after Supreme Court Aadhaar Verdict: It's Business as Usual, Huffington Post (26-09-2019) available at https://www.huffingtonpost.in/entry/a-year-after-supreme-court-aadhaar-verdict-its-business-as-usual_in_5d8c69a8e4b0ac3cdda340cc last visited 10 June, 2020.

[22]Megha Mandavia, Aarogya Setu app not mandatory for air, rail travel: Centre to Karnataka HC, Economic Times, 12-06-2020 https://economictimes.indiatimes.com/news/politics-and-nation/aarogya-setu-app-not-mandatory-for-air-rail-travel-centre-to-karnataka-hc/articleshow/76343053.cms#:~:text=BENGALURU%3A%20The%20Central%20Government%20on,that%20its%20use%20was%20voluntary. last visited 18 June, 2020.

[23]Jagriti Chandra, Airlines make Aarogya Setu mandatory, The Hindu (24-05-2020), available at https://www.thehindu.com/news/national/airlines-make-aarogya-setu-mandatory/article31652631.ece last visited 10 June, 2020.

[24]Thaler, Richard H. Sunstein, Cass R. Nudge: Improving Decisions About Health, Wealth, And Happiness. New Haven: Yale University Press, 2008.

[25] *Id.*

[26]Christina L. Wissinger, Privacy Literacy: From Theory to Practice, Communications in Information Literacy, Volume 11(2) (2017), available at https://files.eric.ed.gov/fulltext/EJ1166461.pdf, last visited 12 June, 2020 ("digital literacy is the ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and technical skills While privacy literacy definitions focus on the understanding of the responsibilities and risks associated with sharing information online, digital literacy focuses on the task-based use of information in a digital environment. Based on these definitions, privacy literacy aligns more closely with critical thinking").

[27]Berkman Klein Centre, Safety, Privacy, and Digital Citizenship: Introductory Materials, Digital Citizenship Research Platform, available at Christina L. Wissinger, Privacy Literacy: From Theory to Practice, Communications in Information Literacy, Volume 11(2) (2017), available at https://files.eric.ed.gov/fulltext/EJ1166461.pdf, last visited 12 June, 2020, last visited 12 June, 2020; for a definition of privacy literature as compared to digital literacy, see Christina L. Wissinger, Privacy Literacy: From Theory to Practice, Communications in Information Literacy, Volume 11(2) (2017), available at https://files.eric.ed.gov/fulltext/EJ1166461.pdf, last visited 12 June, 2020.

benefits to participating in the system.[28] [29] **(**Table 1 indicates situations in which nudges have oriented people towards using the application. Addressing regulation through nudges by administrative authorities becomes particularly challenging when the operationalization of the framework is discrete and not yet transparent).[30] **Initially, the application was made mandatory for employees. Then, it was made mandatory for traveling on flights. Subsequently, the Standard Operating Protocol was modified making it into an advisory. However, this hybrid combination of regulation followed by a nudge respectively, requires careful examination. Even after changing the nature of the regulation, the push arising from its earlier regulatory characteristic persists.**

Initially announcing something as mandatory and then later announcing that it is recommendatory is an evolved type of 'hybrid regulatory nudge'. Sunstein and Thaler point out in their book that it is significantly more unlikely for people to *opt-out* than to opt-in since opting out requires people to disrupt the status quo and incur some burden or (opportunity) cost in terms of, for instance, time or energy.[31] The essence of the advisory or regulation therefore remains mandatory even after the relaxation. It is in this light that we must view these advisories (The importance of the element of consent, autonomy, and choice fundamentally to dignity and privacy is discussed later in the section on privacy intrusions within the proportionality section).

The ubiquity of the mandate affects access to essential services for a broad range of stakeholders

Having established that the application continues to remain mandatory for all practical purposes, this section explains how this mandate affects a broad range of stakeholders (see table 1 below):

[28]Kumar, Not furnishing PAN or Aadhaar? You won't get this latest benefit announced by Modi govt, Financial Express (15-05-2020), available at https://www.financialexpress.com/pan-card/pan-aadhaar-link-tax-deducted-at-source-tds-tcs-rates-benefit-modi-govt/1959608/ last visited 10 June, 2020.

[29]Theo Wilson, Compulsory Digital Contact Tracing Is Probably Legal, but Still Suboptimal, Jurist (26-04-2020) available at https://www.jurist.org/commentary/2020/04/theo-wilson-compulsory-contact-tracing/ last visited 10 June. 2020.

[30]Hill, A. Why Nudges Coerce: Experimental Evidence on the Architecture of Regulation. *Sci Eng Ethics* 24, 1279–1295 (2018). https://doi.org/10.1007/s11948-017-9944-9.

[31]Thaler, Richard H. Sunstein, Cass R. Nudge: Improving Decisions About Health, Wealth, And Happiness. New Haven: Yale University Press, 2008.

Table 1: Mapping its Ubiquity

SECTORS WHERE AAROGYA SETU IS UBIQUITOUS	NUDGE/INDIRECT MANDATE[32]	RELATIONSHIP WITH POTENTIAL FREEDOMS
Airlines[33]	Even though a clarification was issued by the Aviation Ministry on 22nd May 2020, it is still reported widely in the news that Aarogya Setu is mandatory to board flights. Further clarification has been released clarifying that the mandate is an advisory; however, airlines perhaps in efforts towards being over-cautious continue to keep the application mandatory	**Freedom to travel**
Shramik Trains[34]	"As the Indian Railways announced the commencement of some of its passenger services with the introduction of 15 Special trains, people traveling in the Special trains were asked to download the app before	**Freedom to travel (for particularly vulnerable groups)**

[32]Thaler, Richard H. Sunstein, Cass R. Nudge: Improving Decisions About Health, Wealth, And Happiness. New Haven: Yale University Press, 2008.

[33]Times Now Digital, Aarogya Setu app preferable, not mandatory for air travel: Hardeep Puri clarifies, available at https://www.timesnownews.com/india/article/from-air-to-travel-by-train-list-of-places-where-aarogya-setu-app-is-mandatory/593861 last visited 10 June, 2020.

[34]TimesNowNews, from air to travel by train: List of places where Aarogya Setu app is mandatory, 19-05-2020, available at https://www.timesnownews.com/india/article/from-air-to-travel-by-train-list-of-places-where-aarogya-setu-app-is-mandatory/593861 last visited 10 June, 2020.

	beginning the journey."[35] Even though this mandate has been relaxed to an advisory, digital literacy about this relaxation or the importance of consent is yet to permeate the people at large	
Metro[36]	The Delhi Metro and the Noida Metro Railway Corporation (NMRC) has made it mandatory for commuters to download and use the application whenever the services recommence[37]	**Freedom to travel**
Hotels	Downloading and using Aarogya Setu is a mandatory precondition to booking hotel rooms[38]	**Residence/Hospitality**
Employment	Employers could unilaterally make it mandatory to use Aarogya Setu. There exists no legal framework provided for within the Order that precludes employers from creating such a mandate	**Financial Security**

[35]Times Now News, from air to travel by train: List of places where Aarogya Setu app is mandatory, 19-05-2020, available at https://www.timesnownews.com/india/article/from-air-to-travel-by-train-list-of-places-where-aarogya-setu-app-is-mandatory/593861 last visited 10 June, 2020.

[36]Kriti Bhalla, Aarogya Setu Mandatory For Metro Travellers In Delhi-NCR, 20-05-2020, available at https://www.timesnownews.com/india/article/from-air-to-travel-by-train-list-of-places-where-aarogya-setu-app-is-mandatory/593861, last visited 10 June, 2020.

[37]The Hindu, Commuters must have Aarogya Setu app to board metro: NMRC, 17-05-2020, available at https://www.thehindu.com/news/cities/Delhi/commuters-must-have-aarogya-setu-app-to-board-metro-nmrc/article31605559.ece last visited 18 June, 2020.

[38]Times of India, Planning a Trip to Daman? Book a Hotel First (10-06-2020),available at https://timesofindia.indiatimes.com/city/surat/planning-a-trip-to-daman-book-a-hotel-first/articleshow/76309373.cms last visited 10 June 2020.

Malls	Malls in Hyderabad have made it mandatory to download and display a 'green status' indicating asymptomatic health condition on the Aarogya Setu App	**Subsistence (e.g. food, clothing)**
Parks	The Municipal Corporation of Delhi has allowed jogging on tracks in parks between 7 AM and 7 PM respectively provide visitors use Aarogya Setu	**Public (Respiratory) Health**

Having outlined why the mandate to use the application remains ubiquitous, the next section broadly outlines the operability of the application before finally addressing the privacy concerns through the lens of proportionality

OPERABILITY OF AAROGYA SETU

The application was developed by the National Informatics Commission ('**NIC**') which also controls its operability.[39] Before this G.O, a public address urged the Indian citizenry to use the application to facilitate containment of COVID-19[40] The application witnessed an unprecedented jump of users to 100 million in number in a short span of 41 days.[41]

[39]Jhinuk Sen, Hindustan Times, *Aarogya Setu is mandatory, but still not accessible to people with disabilities* 7-05-2020, available at https://www.hindustantimes.com/tech/aarogya-setu-is-mandatory-but-still-not-accessible-to-people-with-disabilities/story-LBMMEIpYsq3t5Okoa46rfJ.html (Last visited 14-05-2020).

[40]Jagmeet Singh, Aarogya Setu App Download Encouraged by PM Modi, Amid Privacy Concerns Raised by Experts, 14-04-2020, NDTV, https://gadgets.ndtv.com/apps/news/aarogya-setu-app-download-prime-minister-narendra-modi-address-coronavirus-covid-19-india-2211541, last visited 18 June, 2020.

[41]Reuters, ET Telecom News, *Aarogya Setu app coming to Reliance JioPhone soon* 8-05-2020, available at https://telecom.economictimes.indiatimes.com/news/aarogya-setu-app-coming-to-reliance-jiophone-soon/75614707 18 June 2020.

After the G.O, a petition was filed before the Kerala High Court ('KHC') challenging the mandate.[42] The KHC adjourned this petition till 18th May, indicating, "extraordinary times require extraordinary measures".[43] However, the Court sought a statement from the Central Government on measures taken to safeguard privacy concerns arising from data collected using the application.[44] One of the petitions claims that the G.O violates the safeguards stipulated in Justice KS Puttaswamy & Ors. v. Union of India & Anr. ('**Puttaswamy I**')[45] and therefore prays that it be struck down.[46] The Petition seeks a direction to stop taking any coercive steps against persons who do not comply with the impugned G.O.

During the pendency of the aforementioned petitions, by a subsequent Notification dated 11th May, the Government of India introduced the 'Arogya Setu Data Sharing and Knowledge Access Protocol, 2020'[47] ('**The Protocol**') with the view to implement principles of data protection.[48] Subsequently, the source code of the application was released to the public towards increasing transparency in its operability.

The next section acknowledges the limitations of source code transparency followed by a discussion of the privacy policy and the protocol respectively. This is to broadly outline the governing framework of the application before discussing the privacy concerns that stem thereof.

The Code

This section measures the transparency that yields from publicising the source code itself, **acknowledging at the same time the limitations of transparency in addressing privacy concerns**.

---

[42]K.C Gopakumar, Plea in Kerala HC against Centre's directive on Aarogya Setu app, The Hindu, 8-5-2020, available at https://www.thehindu.com/news/national/kerala/plea-in-kerala-hc-against-centres-directve-on-arogya-setu-app/article31535285.ece, last visited 25-05-2020.

[43] Meera Emmanuel, "Extraordinary situations call for extraordinary measures" Kerala HC adjourns plea against mandatory imposition of Aarogya Setu
to May 18, BarandBench 12-05-2020, available at
https://www.barandbench.com/news/litigation/extraordinary-situations-call-for-extraordinary-measures-kerala-hc-adjourns-plea-against-mandatory-imposition-of-aarogya-setu-to-may-18 last visited 29-05-2020

[44] *Id.*

[45] Justice KS Puttaswamy (Retd.) & Ors. v. Union of India & Anr. (2017)10 SCC 1.

[46] *Id.*

[47]Aarogya Setu Application, Data Access and Knowledge Sharing Protocol, 2020, available at https://meity.gov.in/writereaddata/files/Aarogya_Setu_data_access_knowledge_Protocol.pdf (Last visited 14-05-2020).

[48] *Id.*

As already mentioned in the introduction, there exists a **strong public interest in ensuring that the algorithm makes predictions in a manner which is fair, i.e. bereft of any algorithmic biases.** These biases could hurt some groups more than others. In the absence of knowledge about these biases, any consent towards using the Application is not adequately *informed*, and hence not meaningful. **Meaningful algorithmic transparency (if achieved as explained in the 'Recommendations' section of the report) with all its limitations (explained on the next page) can help verify and confirm the absence of these biases.** The public's ability to examine how their data is being processed helps in discerning the consequences of consenting to a system. Opaque decision-making can exacerbate the potential risks of unintended disproportionate impact on some groups more than the others. These consequences could be entirely unintentional, stemming from inadvertently internalized biases[49] inherent in the underlying datasets or predictive models. This is not to say that transparency alone can solve all privacy concerns. **Transparency is only one of the interests that needs to be secured. Transparency is just a means to identify disproportionate intrusions into privacy compromises. Once these concerns are identified, the next step is to alleviate them by creating adequate privacy safeguards** (as explained in the recommendations section). Having said that, this section engages with the *extent* to which the operability of the Application is meaningfully transparent.

At the outset, it is important to flag that in India, litigation centred around the absence of transparency in government-used algorithms is unprecedented. However, a Court in Hague, Netherlands recently invalidated SyRI,[50] a government-used algorithm in welfare due to its opaque operability.[51] Addressing concerns of transparency at an early stage is therefore desirable, since it enables identification of privacy concerns and creates scope for suitable

[49]The three types of bias in predicting the color coding of users or predicting hotspots or other appropriate health responses are broadly (i) input bias, (ii) training bias, and (iii) programming bias. These biases are discussed in detail under the 'openness principle' section of the Report.

[50]NJCM c.s./De Staat der Nederlanden (SyRI), case No. C/09/550982/ HA ZA 18/388 ("6.91. The importance of transparency, in the interest of verifiability, is also compelling, because using the risk model and the analysis that is carried out in that context carries the risk that discriminatory effects – unintentional or otherwise – occur...analysing large data sets, with or without deep learning/self-learning systems is undeniably useful, but may also yield undesirable results, including unjustified exclusion or discrimination"). While it is true that conceptually speaking, Aarogya Setu and SyRI serve different purposes, there are few key commonalities as well. These include (as explained above) similar absence of meaningful algorithmic transparency, exacerbating stigma in zones identified as problematic (in case of SyRI) or red (in case of Aarogya Setu) respectively. The zoning determines access to fundamental freedoms such as movement, employment, etc.

[51]This is just to indicate that transparency became the basis to confirm privacy harm due to disparate impact of the application on vulnerable groups ("Without insight into the risk indicators and the risk model, or at least without further legal safeguards to compensate for this lack of insight, the SyRI legislation provides insufficient points of reference for the conclusion that by using SyRI the interference with the right to respect for private life is always proportionate and therefore necessary").

changes. In the context of Aarogya Setu, releasing the server code in realizing the desirable extent of transparency and therefore addressing this particular privacy concern.

Coming to measure of transparency that the framework governing Aarogya Setu currently offers, the source code[52] was recently made public. However, the source code of the application relates only to the operability of the application on the user's *phone,* and associated vulnerabilities. The processing of user data assisting predictions for appropriate health responses does not take place on the application interface on the user's phone. **The application interface on the user's phone acts as a conduit**: the data is collected from the user's phone (when the user enters the data in her phone). Then it is sent to the Government of India ('**GoI**') server (e.g. whenever the user undergoes a self-assessment which is recommended).[53] The privacy policy suggests that after every self-assessment (e.g. evaluating whether a user tests positive), contact data (defined below in this Brief) is sent to the GoI server. The algorithmic model guiding predictions at the GoI server determines appropriate health responses. The source code, therefore, does not help developers understand the vulnerability of the GoI server which could be relying on a black-box machine-learned model (i.e. the black-box). The black-box makes predictions towards appropriate health responses (which could be riddled with several algorithmic biases). This model, in contrast to the source code which has been made accessible, remains hidden from users.

Further, the datasets that become the basis of processing at the GoI server are also, for obvious reasons, not open-sourced (since doing that itself could raise serious privacy concerns by exposing personal data to vulnerabilities). Once the processing is done, at the GoI server, the predictive outcomes (i.e. processed data) are conducted back to the user's phone in the form of a predictive advisory/visual. In making these predictions, the black box could continue to process demographic data in a manner that is riddled with algorithmic biases.[54] As a result, experts would be inevitably unable to understand why a certain prediction is made (if one reads the privacy policy, the application makes predictions such as "identify emerging areas where infection outbreaks are likely to occur".[55] To put it simply, **the source code deals only with the operability of the application on the device of the user**. **Publicizing the source code helps in identifying cybersecurity vulnerabilities of the user data stored on the application, but neither the user data stored on the GoI server nor insights into**

[52]Aarogya Setu Source Code, available at https://github.com/nic-delhi/AarogyaSetu_Android last visited (29-05-2020).

[53]The technological expertise in relation to the implications of publicising the source code was provided to me by Agrim Mittal, alumnus of Indian Institute of Technology (IIT), Roorkee. No position taken in this paper, however, is attributable to him.

[54]European Parliament, A governance framework for algorithmic accountability and transparency , available at https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf last visite (29-05-2020),

[55]Clause 2(d), Aarogya Setu Privacy Policy, available at https://web.swaraksha.gov.in/ncv19/privacy/, last visited (29-05-2020).

the algorithmic models governing the predictions. The algorithmic model governing predictions that could be riddled with biases (at the GoI server) continues to remain a black box.

It is presently not clear whether the source code can in some way be reverse-engineered to attain more information on the GoI server. It is perhaps also undesirable to expose the GoI server to cybersecurity risks by making its models transparently available. At the same time, as already established, the source code does not ordinarily reveal how data is stored or processed on the GoI server.

In other words, the source code of Aarogya Setu available is different from making the predictive model or algorithm governing the data processing undertaken by the centralized Government of India ('GoI') server (how and when the data is sent to the GoI server is discussed in more detail in the 'privacy policy' section) Further, any disproportionate impact on vulnerable communities is a product of systemic and structural environments that cannot be mitigated merely with greater transparency but requires deeper thought on the patterns of discrimination-which are beyond the remit of this report. As a result, **access to the source code may not result in understanding the logical basis behind several predictions made by the black box or algorithmic model governing predictions made by the processing at the GoI server**.

No doubt, the source code helps address cybersecurity-vulnerabilities of the data stored on the user device by the application; not the data *sent* to the GoI server:

> "In many cases, review of source code can be a powerful form of scrutiny. A code audit, also called "white-box testing" in the computer science field, is an analysis of source code to discover errors. These audits can also include a review of specific system behavior — logs that record data access, calculations, decision trees, and errors. For some automated systems, 'source code' might also refer to the statistical models that rank, sort, classify, and score inputs. Models can be more difficult to review than descriptive, deterministic computer code, but in some cases (usually those that rely on a limited number of factors), understanding how different inputs are weighted in an algorithm can be illuminating"[56]

[56]Omidyar Network, *Public Scrutiny of Algorithmic Networks, available at https://www.omidyar.com/sites/default/files/file_archive/Public%20Scrutiny%20of%20Automated%20Decisions.pdf* ;("knowledge of a system's existence, purpose, impact, constitution, policies, inputs and outputs, and training data can be helpful to both scrutinize and govern these systems. This framework highlights how nontechnical insights about an automated system can be just as important, and often more important, than its technical, tangible artifacts").

This is perhaps why the Government of France has recently made it mandatory for itself to make source codes of government-used algorithms available.[57] It has recognized that source codes constitute 'public records' which must be mandatorily accessible (except when disclosure can impact the integrity of government security systems).[58]

The following paragraph sums up the limitations of publicizing the source code:

> "Key issues are complexity (linked to the scale of data, the modularity of algorithms, iterative processing and randomized tiebreaking), the interconnection of decisions, and processes that are learned from data. As a result of these issues, simply releasing the source code of an algorithmic system would often not provide meaningful transparency. There are also other reasons why simply releasing a model (or the learning algorithm and the data) is often not a feasible solution to transparency: data privacy could be compromised since it may be possible to 'reverse engineer' a model to determine the data used to construct it; continuous, or frequently updated, learning to capture and incorporate new data and changing trends also poses a challenge."[59]

To sum up this section: in the absence of adequate information about the predictive models used by the GoI servers and the training data used to build these models, it may not be possible to examine the algorithmic biases which guide the appropriateness of health-related responses predicted by Aarogya Setu.

Privacy Policy

Once the user opens the application, they receive a recommendation to keep their phone location data and Bluetooth switched-on at all times to continuously track every place an individual has travelled to at intervals of fifteen minutes.[60]

---

[57] *Id.*

[58] *Id.*

[59] European Parliament, A governance framework for algorithmic accountability and transparency , available at https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf,

[60] Economic Times, *How to use Aarogya Setu app and find out if you have coronavirus symptoms* (April 15, 2020), https://economictimes.indiatimes.com/tech/software/how-to-use-aarogya-setu-app-and-find-out-if-you-have-covid-19-symptoms/articleshow/75023152.cms (Last visited 14-05-2020).

Broadly, according to the privacy policy, the application collects two categories of information. Allow me to refer to them as static and dynamic (both these categories of datasets are subject to different restrictions).

The static component, i.e. the information which remains relatively constant, is collected at the time of registration. This includes the **user name, phone number, age, sex, profession, and list of countries visited in the past 30 days**.[61] This information, **according to an earlier version of the privacy policy is collected, hashed** and stored in the form of a unique ID in a server that is controlled by a Government of India server.[62] Notably, according to this version, the hashing takes place only for this category of datasets. However, **the subsequent privacy policy does not outline 'hashing' as the standard of anonymization**. The privacy policy does not further outline the standard of anonymization, the capabilities of the server, the entities which have access to the server. The most recent privacy policy[63] of the application does not seem to mention hashing as the standard of anonymization that the data at the GoI server is subjected to. The standard of anonymization is not mentioned in the policy.

The Article 29 Working Party in its report on 'Anonymisation Techniques' pointed out that **hashing is not an *anonymization* technique (i.e. a technique which makes an individual close to irreversibly unidentifiable); hashing is only a technique of 'pseudonymization', a significantly lower and risk-prone method of undermining linkability**.[64] This is because, in *hashing*, the information is passed through a hash algorithm (i.e. a function) which translates the input data (e.g. health data) into a hashed output, generally a string of characters. The output for a particular input data necessarily corresponds to a particular input; so if an attacker is fully aware of the entire possible range of information (e.g. mobile numbers) at one end, identifiability (with the hashed output) is not very difficult at all.[65] Since our mobile phone numbers are generally available in public databases (including grocery stores, malls, pharmacies, etc), i.e. practically any place where we make a purchase, it may not re-identification may be possible consequent to a brute force attack.

---

[61] Aarogya Setu Application, Privacy Policy, Clause 1(a), available at https://web.swaraksha.gov.in/ncv19/privacy/ (Last visited 14-05-2020).

[62] *Id.*

[63] *Id*; Old Privacy Policy, available at https://web.archive.org/web/20200414082653/https:/web.swaraksha.gov.in/ncv19/privacy/; ("This information stored on the Server will be hashed with a unique digital id (DiD) that is pushed to your App"). The statement on hashing has been removed in the revised Privacy Policy. For a detailed discussion, see Aarogya Setu Old and New Privacy Policy, MediaNama, available at https://www.medianama.com/wp-content/uploads/Aarogya-Setu-Privacy-Policies-Comparison.pdf last visited 18 June, 2020.

[64] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf last visited 18 June, 2020.

[65] *Id.*

Second, the dynamic component of the information includes records of Geo-Positioning System or Cell-Site Location Information ('CSLI') of users individually. It also includes information obtained through Bluetooth-to-Bluetooth interactions between two users at a time when they cross each other within a particular range. This information is collected to trace the information regarding the time and location at which the contact takes place. The information, according to the policy, is then stored 'securely' on the server; however, the policy does not specify the safeguards for secure storage of this information. This becomes important since we need to better understand the standard of security that location information needs to receive in the broader context of its relationship with the right to privacy. The standard of security for the dynamic component, unlike the static component, is not specified in the privacy policy.

The Protocol

The protocol supplements and does not substitute the existing privacy policy of the application. The protocol only lays down broad principles of data protection which govern its operability. This is made further clear by paragraph 5 of the protocol.[66]

The protocol broadly defines all the data collected by the application which includes contact data, demographic data, and self-assessment data as 'response data'. To reference specific definitions:[67]

1. "Demographic data means the name, mobile number, age, gender, profession, and travel history of an individual.
2. Contact data means data about any other individual that a given individual has come near, including the duration of the contact, the proximate distance between the individuals, and the geographical location at which the contact occurred.
3. Self-assessment data means the responses provided by that individual to the self-assessment test administered within the Aarogya Setu mobile application. Location data means data about the geographical position of an individual in latitude and longitude"[68]

Having provided an overview of the framework governing the operability of the application, the next section explains why collection of location data by Aarogya Setu can result in a privacy compromise.

[66] Aarogya Setu Application, Data Access and Knowledge Sharing Protocol, 2020, available at https://meity.gov.in/writereaddata/files/Aarogya_Setu_data_access_knowledge_Protocol.pdf (Last visited 14-05-2020).

[67] *Id.*

[68] *Id.*

Reasonable expectation of privacy over location data

In order for there to be a privacy intrusion in the first place, the mandate needs to affect a reasonable expectation of privacy.[69] The existing legal framework recognizes that there exists an expectation of privacy over demographic data.[70] However, as already established (see 'the protocol' section) **the application collects not just demographic data but even other types of response data, including inter alia location data** (i.e. contact data as defined in the protocol). In the Indian context, the contours of a reasonable expectation of privacy over location data are not clear.

A cell phone's location can be detected through cell site location information (CSLI) or global positioning system (GPS) data.[71] CSLI refers to the information collected when a cell phone figures out its location to nearby cell towers. CSLI from cell towers nearby facilitates identifying the approximate location of an individual. If one has information from multiple cell towers, an individual can be located with great precision, through a process known as 'triangulation'.[72] The GPS capabilities of a user's cell-phone make it possible to track an individual within a range of five to ten feet. The cell phone information of an individual could be either prospective or historical.[73] Prospective data makes it possible for the Government

[69]2017 (10) SCC 1.

[70]Section 13, Aadhaar and Other Laws (Amendment) Act, 2019, available at https://uidai.gov.in/images/news/Amendment_Act_2019.pdf last visited (29-05-2020); The provision included (within section 29 of the original legislation) demographic information alongside core biometric information within the scope of safeguards against public disclosure see Appendix, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, available at https://www.thehinducentre.com/resources/article24561547.ece/binary/Data_Protection_Committee_Report-comp, last visited (29-05-2020) ('29. Restriction on sharing information— (4) No Aadhaar number, demographic information or photograph collected or created under this Act in respect of an Aadhaar number holder shall be published, displayed or posted publicly, except for purposes, if any, as may be specified").

[71]Eric Lode, *Validity of Use of Cellular Telephone or Tower to Track Prospective, Real Time, or Historical Position of Possessor of Phone Under Fourth Amendment*, 92 A.L.R. Fed. 2d 1 (2015); See also University of California, Berkeley, *Cell Phone Location Tracking, A National Association of Criminal Defense Lawyers (NACDL) Primer*, available at https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-06-07_Cell-Tracking-Primer_Final.pdf (Last visited 14-05-2020).

[72]The Quint, *Here's How Aarogya Setu COVID-19 Tracker Works on Non-Smartphones* (May 12, 2020), available at https://www.thequint.com/tech-and-auto/tech-news/this-is-how-aarogya-setu-can-work-on-non-smartphones (Last visited 14-05-2020).

[73] *Id.*

to track an individual's movement in real-time. Historical data provides historical information about an individual's past movement or travel which helps in piecing together past events to make sense of an individual's movement. **For digital contact tracing, both these categories of information are collected and retained (since prospective data accumulates and becomes historical data over a sustained period)**.

Does an individual exercise a reasonable expectation of privacy against being subjected to real-time location tracking? To answer this question, one would need to reimagine parts of what was held in *Kharak Singh*[74] and *Govind* in light of *Puttaswamy*.

In *Kharak Singh*, the majority among six judges held that sub-sections of the Uttar Pradesh Police Regulations which empowered the police to track the physical movement of a history-sheeter is a reasonable restriction on an individual's personal liberty. *Kharak Singh* also of course held that unwarranted domiciliary visits undermine an individual's personal liberty, a fundamental right forming part of Article 21 of the Constitution. The U.P Regulation 236 reads as follows[75]:

> "U.P Regulation 236 under the Police Act:[76] "Without prejudice to the right of Superintendents of Police to put into practice any legal measures, such as shadowing in cities, by which they find they can keep in touch with suspects in particular localities or special circumstances, surveillance may for most practical purposes be defined as consisting of one or more of the following measures :
> (a) Secret picketing of the house or approaches to the house of suspects;
> (b) domiciliary visits at night;
> **(c) through periodical inquiries by officers not below the rank of Sub-Inspector into repute, habits, associations, income, expenses, and occupation;**
> **(d) the reporting by constables and chowkidars of movements and absence from home;**
> **(e) the verification of movements and absences by means of inquiry slips;**
> (f) the collection and record on a history- sheet of all information bearing on conduct."[77]

The Court treated clause (b) on the one hand and clauses (c), (d) and (e) (i.e. the three together) separately, i.e.:

1) domiciliary visits to the Kharak Singh's house[78] and
2) Watching of physical movement outside the claimant's house (in public spaces).[79]

---

[74] Kharak Singh v. State of Uttar Pradesh & Ors., AIR 1963 SC 1295.
[75] *Id.*
[76] Indian Police Act, 1861.
[77] Kharak Singh v. State of U.P & Ors., 1963 AIR 1295.
[78] *Id*.
[79] *Id.*

With respect to the former (i.e. domiciliary visits), the majority held that they violate personal liberty. **The Court seemed to implicitly conceptualize the right to privacy in terms of personal liberty in a properterian sense** (i.e. liberty ends where the home ends).[80] The Court recognized that a person's house is their castle, but was unwilling to extend this principle to their *person,* as they move outside their homes (in public spaces). This properterian conception of privacy[81], however, was many years later rejected by the Supreme Court of India in *District Registrar and Collector v. Canara Bank* ('***Canara Bank***').[82] In *Canara Bank*, a provision of the Stamp Act was under challenge which gave wide powers to the Collector to authorize searches of documents submitted by customers to banks.[83] The Court rejected the third-party doctrine which was formulated in *United States v. Miller.*[84]

In Miller, the Court had held that to conduct searches (i.e. inspection) via third parties (e.g. a third party bank which holds records of a customer), there is no requirement of a warrant since there is a reduced reasonable expectation of privacy over information knowingly shared with third parties,i.e. the public.[85] The Supreme Court cited Lawrence Tribe's criticism of the properterian conception of privacy and his famous conception of privacy as a right which 'rests with persons and not places'.[86] (Surprisingly, the Miller test continues to exist in the United States, since *Carpenter* (discussed later in this report) distinguished collection of cell-site location information from telecom companies from seeking information from banks as third-parties as in the case of *Miller*. The former, according to *Carpenter*, is significantly more intrusive and therefore raises a reasonable expectation of privacy; this is a distinction which was not made by the Court in *Carpenter*) (at the time of *Kharak Singh*, the inter-relationship of rights was subsequently recognized in *R.C Cooper*[87] and *Maneka Gandhi*[88] respectively was not recognized and judges at that time were fairly positivist and against reading in unenumerated rights into enumerated rights).

---

[80] Katz v. United States, 389 U.S. 347 (1967).

[81] Richard Alexander, *Privacy, Banking Records and Supreme Court: A Before and After Look at Miller*, South West University Law Review (1978) 10.

[82] District Registrar and Collector v. Canara Bank, (2005) 1 SCC 496.

[83] *Id.*

[84] United States v. Miller, 425 U.S. 435 (1976); For a detailed analysis, see Canara Bank ("the US Supreme Court held that once the documents reached the hands of a third party Bank, the Respondent ceased to possess any Fourth Amendment interest in the Bank record over which there was no legitimate 'expectation of privacy' (as stated in Katz) in the contents of the original cheques and deposit slips, since the cheques were "not confidential communications" but negotiable instruments to be used in commercial transactions and the documents contained only information voluntarily conveyed to the Banks which was exposed to the employees in the ordinary course of business. The Court laid down a new principle of "assumption of risk". It said the "depositor takes the risk, in revealing his affairs to another.")

[85] Carpenter v. United States, No. 16-402, 585 U.S. (2018).

[86] Katz v. United States (1967) 389 US 347; See also Lawrence H. Tribe, 'American Constitutional Law', at p. 1306 (2nd Ed, 1988).

[87] (1970) 1 SCC 248.

[88] (1978) 1 SCC 248.

In Puttaswamy I[89] the settled position (laid down in *Canara Bank*), that privacy rests with *persons* and not places was reiterated.[90] An individual has a reasonable expectation of privacy in public places. Therefore, an individual can exercise privacy even when moving in public. The movement of an individual is an aspect that an individual may reasonably want to hide from the public or the state, for a variety of reasons. This includes the kind of harm that can be caused if an individual's every movement can be tracked.[91] The reasonable expectation of privacy has two components, i.e. the objective component (i.e. whether the society contextually regards tracking of physical movement in public spaces to constitute part of a reasonable expectation of privacy) and the subjective component (i.e. whether one personally endorses this opinion). Both the objective and subjective expectations must be satisfied to raise a claim of privacy in a public context.

Helena Nissenbaum in her 'Theory of Contextual Integrity'[92] highlights that the extent of privacy exercised in public depends on the context. Nissenbaum suggests that labeling information as exclusively public or private fails to take into account the context which rationalizes the desire of the individual to exercise her privacy in public. To explain this with an illustration, there exists a reasonable expectation of privacy in the restroom of a restaurant, even though it is in a public space.[93] Depending on the context, an individual may be willing to share a limited amount of information about their daily travel (to a limited extent). This is because cumulatively, location data can reveal a lot more about an individual than they would be willing to reveal ordinarily to the public or the state:

> "Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly churchgoer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts."[94]

---

[89] Justice KS Puttaswamy (Retd.) & Ors. v. Union of India & Anr. (2017) 10 SCC 1.

[90] *Id*

[91] Neil Richards, *The Dangers of Surveillance*, Harvard Law Review 126 (1934) (2012); Daniel Solove, *A Taxonomy of Privacy*, University of Pennsylvania Law Review 154(3) (2006), available at https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477 (2006).pdf (Last visited 12-05-2020).

[92] Helen Nissenbaum, *Privacy as contextual integrity*, Wash. L. Rev. 79(119) (2004), available at https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf (Last visited 14-05-2020).

[93] *Id.*

[94] In fact, the majority in Puttaswamy II explicitly acknowledged United States v. Jones in the context of discussion on an expectation of privacy against GPS tracking; David Gray, Danielle Keats Citron, *A*

To put it simply, **if Courts today were to rewrite *Kharak Singh*, and determine the constitutionality of the U.P Regulations which enabled physical tracking of an individual in public spaces, the outcome would perhaps be different.** The Court in *Kharak Singh* would (today) hold that tracking an individual's movement even in public spaces affects their liberty and raises an expectation of privacy (since it is being reimagined in after *Puttaswamy*). Courts could further borrow from one of the most recent decisions on the expectation that location information raises: *Carpenter v. the United States* (‘***Carpenter***’).[95] In *Carpenter*, the Supreme Court of the United States held that the FBI's request for cell-site location information (CSLI) of Timothy Carpenter over a sustained period from a telecommunication company constitutes a ‘search’ within the meaning of the Fourth Amendment to the U.S Constitution; that there exists a reasonable expectation of privacy against third parties necessitating a warrant to precede such a search. The Court in Carpenter held that the warrantless search of Carpenter's CSLI constituted a violation of the Fourth Amendment right. The observation that a reasonable expectation of privacy exists over historical cell-site location information in Carpenter is relevant for both historical and prospective cell-site location information that is collected in the course of using Aarogya Setu.

To sum up, there exists a reasonable expectation of privacy over location data and its collection constitutes a privacy compromise. The next section conducts a detailed proportionality review of the application to understand its overall privacy implications keeping in mind the interest of public health.

Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy, NCJL & Tech. 14 (381) (2012); See Arindrajit Basu, Siddharth Sonkar, *Automated Facial Recognition Systems and the Mosaic Theory of Privacy: the Way Forward* (Jan 02,2020), available at https://cis-india.org/internet-governance/automated-facial-recognition-systems-and-the-mosaic-theory-of-privacy-the-way-forward (Last visited 14-05-2020) (“In *United States v. Jones*, the United States Supreme Court had observed that the insertion of a global positioning system into Antoine Jones' Jeep in the absence of a warrant and without his consent invaded his privacy, entitling him to Fourth Amendment Protection. In this case, the movement of Jones' vehicle was monitored for a period of twenty-eight days. Five concurring opinions in Jones acknowledges that aggregated and extensive surveillance is capable of violating the reasonable expectation of privacy irrespective of whether or not surveillance has taken place in public.”); for a detailed explanation see Orin S. Kerr, The Mosaic Theory of the Fourth Amendment, 111 Mich. L. Rev. 311 (2012); Jones (“People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers”).
Available at: https://repository.law.umich.edu/mlr/vol111/iss3/1 last visited (30-05-2020).

[95] Carpenter v. United States, No. 16-402, 585 U.S. (2018).

THE PROPORTIONALITY TEST

Since there is a reasonable expectation of privacy over location data (along with demographic and other data as defined by the combined reading of the privacy policy and the Protocol, of course)[96] it becomes important to examine whether an intrusion into the right (by mandating the use of the application) amounts to a constitutionally permissible restriction. The plurality opinion of four judges of the Supreme Court in Puttaswamy I seemed to favor a three-part test to determine the lawfulness of a restriction to the fundamental right to privacy:[97]

1. There must be a 'law'
2. the law must serve a legitimate state interest
3. The law must be suitably proportionate[98], i.e. there must be a rational nexus between the law and the interest (a detailed discussion on the further modification of this test in the context of Puttaswamy is discussed in the proportionality context)

The three-part test initially conceived in Puttaswamy I requires that first that there must exist a valid law which justifies intruding into the right to privacy. Second, there must exist a legitimate state aim (which Justice Chelameswar in his separate opinion required to be a 'compelling public interest' under certain unspecified circumstances depending on the nature of intrusion).[99] Third, the restriction must be proportionate to the purpose of the law. [100] The next section discusses each prong of the test in great detail to understand how the courts *may* end up applying it to the application practically speaking (with an extended discussion on how the proportionality test has eventually been applied subsequently); and

[96]The focus here is location data since in the context of Aarogya Setu, the sheer *extent* of location data collected and retained has relatively greater implications than other types of information collected (i.e. by itself).

[97]Vrinda Bhandari, Amba Kak, Smriti Parsheera, Faiza Rahman, *An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict*, IndraStra Global 11, available at https://www.ssoar.info/ssoar/bitstream/handle/document/54766/ssoar-indrastraglobal-2017-11-bhandari_et_al-An_Analysis_of_Puttaswamy_The.pdf?sequence=1 (Last visited 13-05-2020).

[98]Rahul Matthan, Privacy 3.0: Unlocking our Data Driven Future, 152 (2018).

[99]Vrinda Bhandari, Amba Kak, Smriti Parsheera, Faiza Rahman, *An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict*, IndraStra Global 11, available at https://www.ssoar.info/ssoar/bitstream/handle/document/54766/ssoar-indrastraglobal-2017-11-bhandari_et_al-An_Analysis_of_Puttaswamy_The.pdf?sequence=1 (Last visited 13-05-2020).

[100] Puttaswamy II, ¶572.

how the courts *should* end up applying the test to review the constitutionality of the application.

This three-part test was subsequently modified in Puttaswamy II v. Union of India and broken down further into a more detailed four-part structured test as explained below.

At the same time, different judges in different contexts have applied different standards and intensities of judicial review to different privacy intrusions. before conducting the proportionality analysis therefore, this report maps the variability of the standard and intensity of review, followed by a justification of why it prefers a four-part structured test over other standards.

Standard and intensity of review

Before a detailed analysis of how the application fairs in respect of the proportionality test, it is important to ascertain the desirable intensity of the substantive and evidentiary standards of judicial review.[101] Ascertaining the substantive standard involves determining the conditions (i.e. e.g. necessity) the fulfilment of which would mean that an intrusion is proportionate. Determining the evidentiary standard involves ascertaining the quality, standard and burden of evidence respectively the fulfilment of which would be necessary to prove that the intrusion is substantively proportionate. As pointed out, different courts have applied the standards of proportionality differently.[102] Determining the standard of proportionality requires an inquiry into the conditions that must be satisfied to determine proportionality of the application (e.g. whether a three or a four-part test). Determining the intensity of review on the other hand involves an inquiry into the extent to which the court would be willing to exercise deference towards the executive prerogative.[103] Knowing the desirable standard and intensity respectively of proportionality helps in measuring the extent by which constructive changes need to be introduced towards satisfying this threshold.

Standards

[101]Paul Craig, 'Proportionality and Constitutional Review' (2020) 3(2) U of OxHRHJ 87 ("if a court is minded to engage in intensive substantive proportionality review it will be more minded to demand more evidence to substantiate the contested decision. By the same token, the more evidence that is seen by the court, the greater the likelihood that it will feel that it has the information from which to make an informed decision on the substance of the case").

[102]Dr. Aparna Chandra, 'Proportionality in India: A Bridge to Nowhere' (2020) 3(2) U of OxHRH J 55; Table 1 indicates the variability in standard of proportionality review across different cases.

[103]Dr. Aparna Chandra, 'Proportionality in India: A Bridge to Nowhere' (2020) 3(2) U of OxHRH J 55.

Dr. Aparna Chandra's work titled '*Proportionality: 'A Bridge to Nowhere*'[104] extensively maps how different courts have applied the proportionality standards with different degrees of intensity. She points out that the variability of the intensity of review based on contextual factors.[105] Dr. Chandra makes two sets of comparisons to characterize proportionality as bereft of any guaranteed degree of intensity.[106] First, Dr. Chandra compares the standards applied by the majority of judges on the one hand and Justice Chandrachud's minority opinion on the other in Puttaswamy II respectively. Then, she compares different approaches adopted by Justice Chandrachud in the plurality opinion in Puttaswamy I and the minority opinion in Puttaswamy II respectively. The comparison yields two significant conclusions:

1. First, **the plurality opinion in Puttaswamy I has conceptualized a significantly lower standard of proportionality in Puttaswamy I that only requires a rational nexus between the object of the restriction and the restriction itself.**[107] In Puttaswamy II, however, the minority opinion has conceptualized a far more rigorous standard of proportionality, where the restriction has to be in its least intrusive form (this would mean that the onus is on the government to explain why particularly Aarogya Setu is the minimally intrusive way of implement digital contact tracing. This may require a comparison of the application with alternatives that are considered to be consistent with best international practices to understand what are available range of options).[108]
2. Second, the majority in Puttaswamy II applied a similarly rigorous standard of judicial review with great intensity while striking down the mandate to inter alia link Aadhaar with bank accounts. However, the majority falls short of applying the same standard of proportionality with the same degree of intensity in examining the constitutional validity of the privacy-welfare trade-off.[109]

At present, therefore, **the precise intensity with which courts would review the proportionality of Aarogya Setu is not clear. Notably, in both situations, i.e. the mandate to use Aarogya Setu and the mandate to link Aadhaar with bank accounts, the criticality of interests urged before the court by the State (i.e. public health and prevention of financial misappropriation respectively) are to a certain extent similar (in terms of gravity), warranting public interest (albeit of a relatively varying degree of intensity).**

---

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *Id*; Divij Joshi, Welfare Automation in the Shadow of the Indian Constitution, Socio-Legal Review (7-02-2020), available at https://www.sociolegalreview.com/post/welfare-automation-in-the-shadow-of-the-indian-constitution last visited 14 June, 2020.

The variability in the standard of assessing proportionality is indicated below in table 2 (this is only an indicative and not an exhaustive table):

Table 2: Variability in Intensity of Proportionality Review

*[110]	**OPINION**	**JUDGMENT**	**STANDARD**	**INTENSITY OF REVIEW**
I	Plurality Opinion, Justice D.Y Chandrachud, Kehar, Agarwal, Nazeer	Puttaswamy I	Reasonableness	Rational nexus between means and end (i.e. does not adopt narrow tailoring eventually)
II	Justice Kaul's separate but concurring opinion	Puttaswamy I	Narrow Tailoring	The specifications of the test could be more adequately clarified The extent of intrusion must be proportionate to the need
III	Justice Chelameswar's separate but concurring opinion	Puttaswamy I	Compelling Public Interest Test (from Govind) under some circumstances Further subject to rights review	Did not clarify under what precise circumstances this test is to be applied If the intrusion affects one of the rights articulated under Article 19, the conditions thereunder

[110]This table attempts to depict the analysis done by Dr. Aparna Chandra's in her paper titled ''Proportionality in India: A Bridge to Nowhere' which helps understand the range of ways in which proportionality has been applied in India. For a detailed explanation, see Dr. Aparna Chandra, 'Proportionality in India: A Bridge to Nowhere' (2020) 3(2) U of OxHRH J 55. This is only for the sake of comparison.

			under Article 19 restrictions	also need to be satisfied
IV	Justice Sapre	Puttaswamy I	Social, moral and compelling public interest	"The State can impose reasonable restrictions on the right to privacy "based on social, moral and compelling public interest following the law"[111]
V	Justice Sikri' opinion on behalf of the majority	Puttaswamy II	David Bilchitz Hybrid: Combination of German and Canadian Tests	"First, identify a **range of possible alternatives** to the measure employed by the State a. Next, examine the **effectiveness of each of these measures** in realizing the purpose in a 'real and substantial manner;' b. Next, examine the **impact of each measure** on the right at stake; c. Finally, determine whether there exists a **preferable alternative** that realizes the aim in a real and substantial manner but is less intrusive on the right as compared to the State's measure."[112]
VI	Justice D.Y	Puttaswamy II	Narrow Tailoring	The intrusion must be the

[111]Vrinda Bhandari, Amba Kak, Smriti Parsheera, Faiza Rahman, *An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict*, IndraStra Global 11, available at https://www.ssoar.info/ssoar/bitstream/handle/document/54766/ssoar-indrastraglobal-2017-11-bhandari_et_al-An_Analysis_of_Puttaswamy_The.pdf?sequence=1 (Last visited 13-05-2020).

[112]Dr. Aparna Chandra, 'Proportionality in India: A Bridge to Nowhere' (2020) 3(2) U of OxHRH J 55.

	Chandrachud			least restrictive way of attaining the end
VII	Justice Sinha	Anuj Garg v. Hotel Association of India[113]	Proportionality	Proportionality between means and ends was to be judged on 'a standard capable of being called reasonable in modern democratic society.'
VIII	Justice Sikri	Modern Dental College and Research Centre v State of Madhya Pradesh[114]	"Structured four-part proportionality test"[115] (a) A measure restricting a right must have a legitimate goal (legitimate goal stage). (b) It must be a suitable means of furthering this goal (suitability or rationale connection stage). (c) There must not be any less restrictive but equally effective alternative (necessity stage). (d) The measure must not have a disproportionate impact on the right holder (balancing stage).	"'the larger public interest warrants such a measure' since various malpractices had been noticed when private institutions were conducting entrance examinations themselves. On this basis, the Court concluded that the restrictions satisfied the test of proportionality, without engaging in either a structured analysis or even examining whether less restrictive means could have been adopted"

[113] (2008) 3 SCC 1; *Id.*

[114] (2016) 7 SCC 353, paragraphs 64 and 65; Supra note 112.

[115] *Id.*

		State of Madras vs. VG Row[116]	Reasonableness	The nature of the right alleged to have been infringed, the underlying purpose of the restrictions imposed, the extent and urgency of the evil sought to be remedied thereby, the disproportion of the imposition, the prevailing conditions at the time

With respect to the evidentiary standard, the intensity with which courts would scrutinise the evidence corroborating the efficacy of the application is not clear. Further, whether the burden to produce this evidence would be imposed on the Petitioners or the State is also not clear, given the manner in which it shifted depending on the context in Puttaswamy II. In Puttaswamy II, as Dr. Chandra points out the evidentiary burden was imposed on the Petitioners in the context of the privacy-welfare trade-off.[117] However, the burden shifted to the State in the context of a universal, (facially) class-neutral[118] obligation to link Aadhaar with bank accounts. As indicated by table 1, the indirect mandate to use Aarogya Setu is ubiquitous, similar to the mandates to link bank accounts and SIM cards respectively in the Aadhaar context. Consequently, courts may be more willing to shift the burden to prove that Aarogya Setu is proportionate, on the state, creating further incentive to conduct a review of its efficacy (periodically).

Suggested Intensity of Review

As pointed out above, courts may review proportionality with a degree of intensity analogous to that in reviewing the mandate to link Aadhaar with bank accounts. **The ubiquitous nature (as explained by table 1) of the application (similar to the mandate to link sim cards unlike a narrower mandate which targets for instance, only welfare recipients) may influence the intensity with which courts review its suitability. Therefore, there is a strong incentive to ascertain and publicize the evidentiary basis of the efficacy of the application.**

If courts apply the standard and intensity of proportionality applied to invalidate linking of Aadhaar with Bank accounts to test Aarogya Setu, privacy incursions would have to be

[116] AIR 1952 SC 196; Supra note 89.

[117] *Id.*

[118] The term class-neutral is loosely used to denote the absence of specificity (e.g. beneficiaries) in the mandate to link bank accounts. A broader discussion on the disparate impact and the relationship between privacy and equality is beyond the scope of this report.

minimally intrusive. It is hoped that the review of the application takes place with the same intensity while considering evidence corroborating privacy harms arising from the application.

Of course, there could be a host of factors relevant to determining the appropriate standard and intensity of proportionality review in a given context. However, the experience from the invalidation of the notifications mandating the linkage of SIM cards and bank accounts respectively indicates that ***ubiquity* is a crucial factor in encouraging a more intense review**. **Consequently. courts may be more willing to apply the structured four-part proportionality test to review Aarogya Setu.** This is because, as indicated by table 1, the use of the application is directly or indirectly mandated in accessing most essential aspects of our lives (e.g. travel, accommodation and employment). However, it is important to acknowledge that at this stage, only an assumption regarding the intensity of the standard of review can be made. Given its ubiquity coupled with the significance of the expectation of privacy over location data (as explained above) along with the types of harm that could result from using the application (discussed in detail in the proportionality analysis) also strengthen the case for a considerably intense review of the substantive (e.g. rights and interests) and the evidentiary aspects[119] respectively.

Roadmap of proportionality analysis

Before discussing each prong of the structured four-part proportionality test, it is important to outline each prong for quick reference:

1. Legality (i.e. the mandate to use Aarogya Setu must be backed by law and there must be a legitimate interest that the means adopted seeks to pursue)
2. Suitability (rational connection between the means and the interest)
3. Necessity (the means adopted must be the least intrusive)
4. Proportionality (the interest overrides the right)

Legality

At present, **there is no clarity as to the extent of specificity required in the valid law which enables a restriction on privacy** (the Aadhaar related orders invalidated for not being backed by law are distinguished from, later in this section). Even in *Kharak Singh,*[120] where the Court was interpreting U.P Police Regulations, the Court admitted that the basis for restricting a

[119]Dr. Aparna Chandra, 'Proportionality in India: A Bridge to Nowhere' (2020) 3(2) U of OxHRH J 55. ("the evidential standards, comprising the burden of proof, standard of proof, and the quality of evidence that have to be fulfilled to prove that the substantive standards have been met or violated").
[120] Kharak Singh v. State of U.P & Ors., AIR 1963 SC 1295.

right under Article 21 needs to have some statutory basis, either statutory law or regulation and cannot be a mere departmental instruction:

> "if the petitioner were able to establish that the impugned regulations constitute an infringement of any of the freedoms guaranteed to him by the Constitution then the only manner in which this violation of the fundamental right could be defended would be by justifying the impugned action by reference to valid law, i.e., **be it a statute, a statutory rule or a statutory regulation**. Though learned counsel for the respondent (i.e. the State) started by attempting such a justification by invoking s. 12 of the Indian Police Act he gave this up and conceded that the regulations contained in Ch. XX had no such statutory basis **but were merely executive or departmental instructions framed for the guidance of the police officers**. They would not, therefore, be 'a law' which the State is entitled to make under the relevant clauses 2 to 6 of Art. 19 to regulate or curtail fundamental rights guaranteed by the several sub-clauses of Art. 19 (1); nor would the same be 'a procedure established by law' within Art. 21"[121]

***Kharak Singh* is therefore not good law to conclude that a restriction under Article 21 requires *anchoring* legislation since the court did not restrict the meaning of valid law to a *parliamentary* legislation per se; the court only extended the meaning of valid law to delegated legislation as well as long as it has the *force* of a law or a statute, i.e. it can be traced to the statutory provision in some way and it satisfied the conditions of a valid delegated legislation** (e.g. **the notification should be reasonably contemplated within the statute itself**).

Subsequently, the court in *Govind* has permitted privacy intrusions (interestingly, in the context of freedom of movement, tracking, and surveillance) by reading a general, enabling provision in a parliamentary law (i.e. the Police Act, 1961) together with delegated legislation (i.e. M.P Police Regulations). In *Govind*, the M.P Regulations which specifically enabled domiciliary visits of history sheeters and tracking their physical movements constituted *delegated* legislation, not a parliamentary law. Yet, the Court upheld the regulations as reasonable, observing that they have the force of law (since the regulations were framed under section 46(2)(c) of the Police Act, 1961. Section 46(2)(c) reads as follows:

> "When the whole or any part of this Act shall have been so extended, the State Government may, from time to time, by notification in the Official Gazette, make rules consistent with this Act--
> (a) to regulate the procedure to be followed by Magistrates and police- officers in the discharge of any duty imposed upon them by or under this Act;
> (b) to prescribe the time, manner and conditions within and under which claims for compensation under section 15A are to be made, the particulars to be stated in such

[121] *Id.*

claims, how the same is to be verified, and the proceedings (including local inquiries if necessary) which are to be taken consequently thereon; and
(c) **generally, for giving effect to the provisions of this Act**."[122]

As can be seen here, **section 46(2)(c) of the Police Act, 1961 is comparably as vague as the provision of the NDMA from which the mandate to use Aarogya Setu was sourced**.[123] Govind was decided after *Kharak Singh* and continues to be a good law to this date (since it was not overruled to any extent in Puttaswamy I and II respectively despite a comprehensive review of all significant cases involving the right to privacy (in fact, if one reads the plurality opinion along with any one of the opinions e.g. Justice Chelameswar who explicitly refers to the 'compelling public interest' as a test to intrude into privacy, one cannot help but reach the conclusion that Govind continues to be good law). *Was Puttaswamy a missed opportunity to question the acceptance of the generality in the Police Act as a valid source of governing law?* Perhaps. Yet, the significance of five judges accepting Govind as good law cannot be disregarded in the face of an observation made in *Kharak Singh* in a compartmentalized manner (on the meaning of 'law' within the context of Article 21).

Arguably, the M.P Regulations (in Govind) are no better than the G.O which enables Aarogya Setu insofar as they both anchor themselves to vague, non-specific statutory provisions as sources of validity. In facts, **courts have proactively enabled location tracking or movement-based surveillance through its orders when there has existed no governing legislation specifically enabling such surveillance**; take, for instance, the recent order of the Delhi High Court granting bail to an accused in match-fixing provided they keep their phone switched on at all times[124] (the court also went ahead to recommend that the Government implement emerging technologies to conduct real-time location tracking of accused on bail) to be tracked; or an earlier order of the Delhi High Court where it mandated the use of facial recognition technology to identify and locate missing children.[125]

Several High Courts across the country have accepted this to be the position. as recently as in 2019, where the Telangana High Court seems to reiterate lawfulness in the context of surveillance of the petitioner's real-time movements based on a 'rowdy sheet':

---

[122] Indian Police Act, 1861, §46(2)(b).

[123]Government Order No. 40-3/2020-DM-I(A), Government of India, Ministry of Home Affairs, available at https://www.india.gov.in/sites/upload_files/npi/files/MHA_%20new_guidelines.pdf last visited 27 May, 2020

[124]State v. Sanjeev Kumar Chawla, CRL. M.C. No. 1468/2020.

[125] Hindustan Times, Unacceptable that Facial Recognition Software Not Bearing Results: Delhi HC, 31-0-2019, available at https://www.hindustantimes.com/delhi-news/unacceptable-that-facial-recognition-software-not-bearing-results-delhi-hc-to-cops/story-YDI7sPs1GdhQTZIr8xwgiI.html#:~:text=The%20Delhi%20High%20Court%20has,last%20three%20years%20remain%20untraced., last visited 10 June, 2020.

> "if police surveillance is per departmental guidelines and not authorized by statute **or rules having statutory force**, it is for the State to prove that the surveillance does not in any way infringe the fundamental rights of the person and the authorities have followed the guidelines scrupulously in ordering surveillance."[126]

The single-judge bench of the Telangana High Court in this decision seemed to be referring to an earlier decision of the Allahabad High Court which also similarly conceived the meaning of law in the context of location-tracking of history sheeters.[127]

At present, there is no clarity as to the extent of specificity that is needed in the anchoring legislation to satisfy the 'valid law' requirement, i.e. the first prong of the three-part test laid down in Puttaswamy I. In both the decisions, i.e. Puttaswamy I and II respectively (as discussed below in this section), there is no binding observation on the extent and scope or the meaning of 'law' generally insofar as the specificity of the provision enabling the privacy intrusion is concerned.

The legality prong of the analysis in Govind (i.e. in the context of location surveillance) did not raise the ire of at least five judges in Puttaswamy I (including Justice Chelameswar). it may be unlikely that the court would hold that Aarogya Setu was contemplated any less under the NDMA than location surveillance as conducted by the police under the M.P Police Regulations. It may not be fair to suggest that reviewing this aspect of Govind may have slipped the mind of the earlier courts; these judgments conduct a very thorough literature review of all significant judgments in India on privacy, with explicit references to Govind multiple times throughout. Based on the permissible extent of generality in parent statute previously, enabling digital contact tracing as an appropriate health response towards containing the Pandemic does not seem disconnected from the scope contemplated by the NDMA.

The idea that for different types of restrictions on privacy, statutory law may or may not be required as a lawful basis is not unusual and has come up in the United Kingdom in several decisions in the United Kingdom including Catt[128] and *Edward Bridges* have specifically

[126]Mohammed Aqeel Ahmed vs The State of Telangana, Writ Petition No. 4587 of 2019 ("In either case-whether the regulation is statutory or non-statutory-domiciliary visits and picketing by the police should be reduced to the clearest cases of danger to community security, and there can be no routine follow-up at the end of a conviction or release from prison in every case").

[127]Sunkara Satyanarayana vs State of Andhra Pradesh, 2000 (1) ALD Cri 117,

[128]R (Catt) v Association of Chief Police Officers, [2015] AC 1065; Even though these cases were decided during the existence of a data protection framework, the absence of a comparable framework has not seriously prejudiced past surveillance measures in India. This is discussed further in this section below.

engaged with this question (discussed below in this section).[129] This question has unfortunately never generally been answered by an Indian Court with great clarity yet (including Justice K.S Puttaswamy & Anr. v. Union of India & Ors.[130] (**'Puttaswamy II'**)) except to some extent in **District Registrar and Collector v. Canara Bank ('Canara Bank')**.[131] While the question of whether non-statutory common law can constitute a basis for imposing some types of privacy restrictions (e.g. CCTVs or facial recognition) is beyond the scope of the report, to mention briefly, in **Canara Bank**[132], the Supreme Court referred to common law as a basis for privacy intrusions as well albeit under limited circumstances[133] In fact, the U.K High Court recently in *R (Bridges) v. C.C.S.W.P.*[134] held that a facial recognition law satisfied the 'lawfulness' test under the European Convention of Human Rights (ECHR) even though it was not based out of any statutory law since common law inheres the police the power to conduct virtual surveillance (e.g. CCTV surveillance[135]) which is not intrusive in a physical sense (e.g. biometrics or DNA):

> "The police did not need statutory powers, e.g. to use CCTV or use body-worn video or traffic or ANPR16 cameras, precisely because these powers were always

[129]Edward Bridges v Chief Constable of South Wales Police, [2019] EWHC 2341, ¶22, available at https://www.judiciary.uk/wp-content/uploads/2019/09/Press-Summary-Bridges-v-Chief-Constable-South-Wales-Police-CO-4085-2018FINAL_-1.pdf (Last visited 13-05-2020), ("…The police did not need statutory powers, e.g. to use CCTV or use body-worn video or traffic or ANPR16 cameras, precisely because these powers were always available to them at common law. Specific statutory powers were needed for e.g. the taking of fingerprints, and DNA swabs to obviate what would otherwise be an assault.")

[130](2019) 1 SCC 1.

[131](2005) 1 SCC 496

[132]*Id.*

[133]*Id* (i.e. Canara Bank); ("Intrusion into privacy may be by - (1) legislative provisions, (2) administrative/executive orders and (3) judicial orders. The legislative intrusions must be tested on the touchstone of reasonableness as guaranteed by the Constitution and for that purpose the Court can go into the proportionality of the intrusion vis-`-vis the purpose sought to be achieved. (2) So far as administrative or executive action is concerned, it has again to be reasonable having regard to the facts and circumstances of the case. (3) As to Judicial warrants, the Court must have sufficient reason to believe that the search or seizure is warranted and it must keep in mind the extent of search or seizure necessary for the protection of the particular state interest. In addition, as stated earlier, common law recognized rare exceptions such as where warrantless searches could be conducted but these must be in good faith, intended to preserve evidence or intended to prevent sudden danger to person or property").

[134]R (Edward Bridges) v. Chief Constable of South Wales Police, [2019] EWHC 2341 (Admin), available at https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf (Last visited 13-05-2020); ("A warrant is required to allow the police to enter someone's private property since otherwise, the act of entering someone's private property without permission would amount to a trespass,. Equally, since the act of taking fingerprints generally requires the cooperation of, or use of force on, the subject and would otherwise amount to an assault, statutory powers were enacted to enable the police to take fingerprints. Both involve physically intrusive acts. By contrast, the use of AFR Locate to obtain biometric information is very different").

[135] *Id.*

> available to them at common law. Specific statutory powers were needed e.g. the taking of fingerprints, and DNA swabs to obviate what would otherwise be an assault."[136]

One could distinguish the holding in Kharak Singh from that in Canara Bank in that the former dealt with domiciliary visits, a type of trespass which is intrusive in a physical sense as opposed to other types of surveillance such as CCTVs or Facial Recognition Systems.[137]

Coming to Puttaswamy II, (I.e. the judgment on the constitutionality of Aadhaar), the Court generally recognized that "in the first instance, any intrusion into the privacy of a person has to be backed by law". At the same time, the Court struck down the mandate to link bank accounts with Aadhaar for not being backed by law:

> "We believe that not only such a circular lacks the backing of a law, but it also fails to meet the requirement of proportionality as well"[138]

However, this observation was made in the context of the absence of any statutory law *at all* that enabled a privacy restriction. This is fairly clear from Justice Bhushan's separate but concurring opinion as well, where his concern seemed to not be the absence of explicit mention in statutory law per se but instead, that there was no statute backing the notification at all.[139] The Court also referred to the meaning of law in the context of Article 13 to include common law powers albeit in a different context.[140] Whether the conception of 'backed by law' in the context of Aadhaar squarely applies in the context of location or health data collected by Aarogya Setu is therefore not clear. This is, as already discussed, primarily for two reasons:

---

[136] *Id.*

[137] Siddharth Sonkar, The Wire, *Is Delhi Police's Use of Facial Recognition to Screen Protesters 'Lawful'?,* available at https://thewire.in/law/facial-recognition-delhi-police-lawful (Last visited 13-05-2020).

[138] (2019) 1 SCC 1 (The circular dated 23.03.2017 at best is only an executive instruction issued on 23.03.2017 by the Ministry of Communications, Department of Telecommunications. The circular does not refer to any statutory provision or statutory base for issuing the circular").

[139] *Id.*

[140] (2019) 1 SCC 1, paragraph 77, (In the context of judicial review of legislation, this provision gives an indication that all laws enforced prior to the commencement of the Constitution can be tested for compliance with the provisions of the Constitution by courts. Such a power is recognized by this Court in *Union of India* v. *SICOM Ltd.* (2009) 2 SCC 121 ('SICOM') In that judgment, it was also held that since the term "laws", as per Article 372, includes common law). The decision in SICOM refers to the common law powers of the crown to recover dues ("A common law which is a law within the meaning of Article 13 of the Constitution is saved in terms of Article 372 thereof. Those principles of common law, thus, which were existing at the time of coming into force of the Constitution of India are saved by reason of the aforementioned provision").

1) the idea of 'backed by law' has been consistent across the aforementioned judgments (including Govind[141])
2) the recent UK HC decision which explicitly validated a non-statutory facial recognition by distinguishing physically intrusive information collection (biometrics (e.g. Aadhaar) or DNA) from *virtual* intrusion

Most surveillance in India happens non-statutorily (e.g. facial recognition[142], use of drones,[143] digital contact tracing across various states[144], etc). **The UKHC ruling hierarchizes between types of surveillance by looking at them granularly**; virtual intrusion (e.g. a CCTV or a facial recognition system) and physical intrusion of biometrics (or DNA is significantly more intrusive, it needs to be backed by statutory law. However, if the data collected is only and only virtual (e.g. location data or facial scan through facial recognition technology) according to the United Kingdom High Court in Edward Bridges, the same need not be backed by a parliamentary law (however, as explained earlier, this position may not be very tenable given that virtual surveillance through location tracking can be equally if not more intrusive)[145].

Courts in India may distinguish between the ruling in the context of notifications invalidated by the majority in Puttaswamy II and the G.O mandating/recommending the use of Aarogya Setu. The majority in Puttaswamy II specifically in the context of the mandatory collection of biometric data and **not all types of privacy intrusion**. **The majority in Puttaswamy II** only distinguished itself from Lokniti Foundation v. Union of India & Anr.[146] (i.e. the order mandating linking of SIM cards with Aadhaar) and observed that the said order did not consider the implications of the mandate on the right to privacy. Surveillance has taken place consistently through non-statutory court orders as well, for instance; which are not backed by any parliamentary law as such, for instance, the recent bail related orders which mandated the use of Aarogya Setu.[147]

---

[141] *Id*.

[142] Supra note 137.

[143] Divij Joshi & Siddharth Sonkar, CoViD-19 Related Digital Surveillance and Tech Measures in India, available at https://docs.google.com/document/d/1L9Lfq67k_u_S6qNQ54784b0FEfJEKb-ecgW5bBI56QY/edit# last visited 10 June, 2020

[144] *Id*.

[145] Supra note 142; Anja Kovacs, When our bodies become data, where does that leave us?, 28-05-2020, available at https://deepdives.in/when-our-bodies-become-data-where-does-that-leave-us-906674f6a969, last visited 14 June, 2020.

[146] (2017) 7 SCC 155.

[147] National Herald India, Bail applicants asked by MPHC to download Aarogya Setu, 21-05-2020 available at https://www.nationalheraldindia.com/india/bail-applicants-asked-by-mp-hc-to-download-aarogya-setu-contribute-to-pm-cares-fund last visited 14 June, 2020.

Finally, it becomes important to consider the minority opinion of Chandrachud J., on the validity of Aadhaar. Here, Justice Chandrachud observed: "an executive notification does not satisfy the requirement of a valid law contemplated under Puttaswamy. A valid law, in this case, would mean a law passed by Parliament, which is just, fair and reasonable. Any encroachment upon the fundamental right cannot be sustained by an executive notification." **However, there is no consensus on whether the meaning of law in Puttaswamy I necessarily refers to a statutory basis and not non-statutory regulation which is sourced from vague parent law, generally (i.e. outside the context of the collection of biometrics for Aadhaar). It may be wrong to assume that the interpretation of 'law' in Justice Chandrachud's minority opinion is the interpretation of the meaning of the law as understood by the majority of the judges in Puttaswamy II.** This is particularly since Justice Chandrachud has divergent views on proportionality in Puttaswamy I and Puttaswamy II respectively). This is also particularly since the judges missed an opportunity to expansively discuss the meaning of 'law' in Puttaswamy I and because it did not overturn Govind insofar as in Govind, the Court held that delegated legislation has the force of law while intruding into the right to privacy. If one is to counter-argue that in Govind, there was a substantial link or nexus between the parent legislation and the delegated legislation (i.e. the Police Act read with the M.P Regulations), this again would be a stretch since section 46(2)(c) is very broadly worded. Therefore, while it has been argued that governing parliamentary law is a prerequisite for mandating the use of the application,[148] courts have read the requirement of 'law' broadly enough to accommodate even general provisions in statutes when reading with delegated legislation that is specific which *is* the case in the context of Aarogya Setu.

It may also be important to note that in Puttaswamy I, Justice Chandrachud in his plurality opinion stressed on the significance of introducing a data protection framework regulating intrusions into informational privacy.[149] However, a privacy intrusion was not strictly preconditioned to the introduction of such a framework as such.

The aforementioned analysis is not aimed at supporting the approach of the court over the years in interpreting the legality prong. It is only to indicate that concerns of executive regulation authorising surveillance being outside the scope of (i.e. ultra vires) a general enabling provision in a parent statute in the context inter alia of location-based surveillance have not raised the ire of courts.

[148]Gautam Bhatia, The Mandatory Imposition of the Aarogya Setu App Has No Legal or Constitutional Basis, The Wire, 4-05-2020 available at https://thewire.in/law/the-mandatory-imposition-of-the-aarogya-setu-app-has-no-legal-or-constitutional-basis last visited 18 June, 2020.

[149]"Formulation of a regime for data protection is a complex exercise which needs to be undertaken by the State after a careful balancing of the requirements of privacy coupled with other values which the protection of data sub-serves together with the legitimate concerns of the State", Per Chandrachud, J., in Puttaswamy, (2017) 10 SCALE 1 at para 179.

It is, *of course*, in the interests of the public to seek that the meaning of 'backed by law' or 'law' is read narrowly to mean only statutory law and not delegated legislation. **Statutory law with adequate degree of specificity is less susceptible to excessive rule-making since it undergoes parliamentary scrutiny and is therefore perhaps a more democratic way to enable surveillance**.[150] Statutory law *explicitly* circumscribing the scope of surveillance also limits the *kind* of restrictions which can be introduced by the executive over the right to privacy. One could counter-argue that in times of the Pandemic and similarly grave situations, it may be difficult to get the Parliament to pass laws that enable surveillance, and the Government may have to fall back on a combined reading of delegated legislation and general statutory provisions delegating rule-making powers. However, fundamental rights such as the right to privacy are too sacrosanct to be subject to the perils of executive indiscretion. **Therefore, a *preferred* interpretation of 'law' in the first-prong of the three-part test would generally be an explicit statutory reference to a type of intrusion as far as reasonably possible. While this may cause administrative inconvenience, the solution is to strengthen our democratic systems, rather than a compromise of the right itself**.

Legitimacy

Broadly speaking, the object of (i.e. interest in) recommending the use of the application is to predict appropriate health responses towards containing the Pandemic.[151] This is primarily achieved with the help of two sets of means. First, by predicting the health status of individual users through colour-coding them according to their risk profiles based on their physical interactions.[152] Second, by predicting emerging hotspots based on the data of individual users cumulatively in specific areas or zones.[153] The two objectives seem closely interrelated in that predicting emerging hotspots depends on accurate prediction of the health status of individual users. At the same time, the precise scope of all the objectives (if any other as well) that the application seeks to cumulatively achieve are not clear given the absence of meaningful algorithmic transparency (for a detailed discussion, see 'the code' section).

---

[150]Siddharth Sonkar, Is Delhi Police' Use of Facial Recognition to Screen Protesters 'Lawful'?, (7 January, 2020) The Wire, available at https://thewire.in/law/facial-recognition-delhi-police-lawful, last visited)April 20, 2020).

[151]Aarogya Setu Application, Data Access and Knowledge Sharing Protocol, 2020, available at https://meity.gov.in/writereaddata/files/Aarogya_Setu_data_access_knowledge_Protocol.pdf (Last visited 14-05-2020).

[152]Mint, Covid-19 contact tracing app Aarogya Setu has alerted 1.4 lakh users: Official, available at https://www.livemint.com/news/india/covid-19-contact-tracing-app-aarogya-setu-has-alerted-1-4-lakh-users-official-11589226902816.html last visited 18 June 2020;

[153] Rhythma Kaul, Aarogya Setu gave forecasts regarding 650 Covid-19 clusters, 10-05-2020, available at last visited https://www.hindustantimes.com/india-news/aarogya-setu-alerted-about-650-clusters/story-1kvGonSkLz77dwH3zMYOQI.html last visited 14 June, 2020; for a detailed excerpt, see supra note 3.

Determining appropriate health responses towards containing the Pandemic is certainly a legitimate interest. In the next section, the report assesses the suitability of the means adopted to attain this interest, which helps us understand whether the operability of the application really and substantially[154] furthers this interest.

Suitability

Before the suitability analysis, it is important to flag that in the Aarogya Setu litigation, inter alia two comparisons in respect of suitability and necessity respectively are crucial. To broadly outline the two: the first comparison involves the examination of the efficacy of digital contact tracing with other methods of containing COVID-19 including manual contact tracing, increased testing, isolation, and a combination of all these methods. The second would involve comparing Aarogya Setu with other applications that have been used internationally to implement digital contact tracing to understand if digital contact tracing, as implemented, is the minimally intrusive way of implementing it. While the second comparison is discussed in detail in the necessity section that follows the discussion on suitability, the first comparison is discussed here, immediately below.

The Protocol suggests that Aarogya Setu is suitable, i.e. to enable appropriate health responses towards containing COVID-19. However, the statistical data justifying such a wide mandate to implement digital contact tracing instead of implementing traditional means of contact tracing is not clear. While several states[155] have encouraged voluntary digital contact tracing, India is currently the *only* country to make it mandatory to use a particular application to facilitate digital contact tracing.

Normally, contact tracing is done through interviews:

> "Contact tracing involves an intensive sequence of difficult and anxiety-laden conversations, and it is the role of a contact tracer to explain how a close contact might have been exposed — while respecting patient privacy — and provide assurance and guidance on next steps. 'A human-out-of-the-loop system will certainly yield better results than having no system at all, but where a competent human-in-the-loop system with

[154] See table 1 for a detailed discussion on the structured proportionality test as applied in Puttaswamy II.
[155]The Hindu Data Team, Data | How safe is Aarogya Setu compared to COVID-19 contact tracing apps of other countries? (19-05-2020) available at https://www.thehindu.com/data/how-safe-is-aarogya-setu-compared-to-contact-tracing-apps-of-other-countries/article31618852.ece last visited 10 June, 2020.

> sufficient capacity exists, we caution against an over-reliance on technology."[156]

However, traditional contact tracing typically done through interviews alone may not be adequate in the context of this Pandemic, because of its highly contagious characteristics.[157] Manual contact tracing is slow and challenging to calibrate at a large scale and increases costs for the Government. Further, it may also be difficult for interviewees to recall strangers encountered during travel.[158]

In a recent report of the Ada Lovelace Institute, it has been argued that there is no clear evidence indicating that contact tracing apps can facilitate the containment of COVID-19.[159] The report explains why apps may not be efficacious in containing the virus for several reasons which raise questions about its suitability:

First, since several people are asymptomatic, it is inherently difficult to track active COVID-19 cases, even though the virus is extremely contagious.[160]

Second, digital contact-tracing is "not very accurate" in determining distance, since it was not built for that purpose. The app can yield 'false positives' or 'false negatives'[161] since physical proximity indicated by the Bluetooth does not necessarily translate into actual physical contact.[162] For instance, the Bluetooth signal of a user living in a thin-walled apartment could indicate that the user has interacted with their neighbor, even if the user has never come in contact with such persons. False positives and negatives, particularly typically over-crowded public spaces (which could typically be a problem given the population density in India) could potentially give people a false sense of reassurance or an exacerbated sense of alarm. Individuals who are more susceptible to being disadvantaged from the inability to verify the potential inaccuracies from the application's predictions also may not have adequate access

---

[156] Jason Bay, Automatic Contact Tracing is not a CoronaVirus, available at Panacea, https://blog.gds-gov.tech/automated-contact-tracing-is-not-a-coronavirus-panacea-57fb3ce61d98 last visited 18 June, 2020.

[157] *Id.*

[158] Ada Lovelace Institute, *COVID-19 Rapid Evidence Review: Exit through the App Store?* (April 20, 2020), available at https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf (Last visited 13-05-2020).

[159] *Id.*

[160] *Id.*

[161] Ashkan Soltani, Ryan Calo, et al., Brookings, Contact Tracing Apps are Not a Solution to the COVID-19 crisis, (April 27, 2020), available at https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/ last visited (29-05-2020).

[162] *Id.*

to smartphones and suffer from relatively greater health inequalities, explained in detail below in the third concern.

Third, persons who are typically susceptible to high risk of contracting the virus generally include the elderly, persons with disabilities or pre-existing conditions, people belonging to marginalized communities (due to poor access to healthcare and proper hygiene facilities).[163] High-risk persons are generally also those who lack either access to smartphones on which contact tracing apps run or the ability to use or navigate the application on a smartphone. This could result in algorithmic bias (discussed in detail under the necessity section) in predicting risk profiles of individuals or emerging hotspots, raising questions about its efficacy and corresponding suitability. **The World Health Organisation has also expressed doubts over the universal efficacy of contact tracing apps, limiting its success to a few anecdotal instances and has emphasized on the need for prior assessment before over-reliance on such techniques: "***Digital tools used for contact tracing should be assessed before use* to ensure safeguarding data protection according to national regulations".[164]

Supplanting traditional methods of contact tracing (as discussed below) entirely (or significantly) with digital contact tracing instead of simultaneously encouraging traditional methods of contact tracing as the primary method of addressing COVID-19 is particularly unsuitable for vulnerable groups (As explained earlier in the absence of meaningful transparency section, a comprehensive review of the applicability of the disparate impact doctrine is beyond the scope of this report). However, this discussion may be relevant while assessing at what scale the use of the application may be suitable).[165] including women, owing to **(a) relatively lower access to smartphones and (b) limited ability to use the application** (as already explained, a comprehensive review of the applicability of the disparate impact doctrine is beyond the scope of this report. **However, this discussion may be relevant while assessing at what scale the use of the application may be suitable**). The recent Harvard Kennedy School's report on the barriers faced by women in accessing mobile phones indicates that there exists a strong community sentiment antagonistic to the idea of phone-ownership by women in rural parts.[166] 47% of women who were able to access a phone in a particular sample were not phone owners but were phone borrowers (dependents)

---

[163] *Id.*

[164] *Id*; see World Health Organization, Contact tracing in the context of COVID-19: interim guidance, 10 May 2020, available at https://apps.who.int/iris/handle/10665/332049 last visited 14 June, 2020.

[165] Marco Johannes Haenssgen, Mobile Phone Diffusion and Rural Healthcare Access in India and China , available at https://ora.ox.ac.uk/objects/uuid:3f48fc8b-5414-4851-926b-07a57eed6cfe/download_file?file_format=pdf&safe_filename=HaenssgenM_Full-Thesis.pdf&type_of_work=Thesis last visited 10 June, 2020; "increasing phone-aided health action threatens to marginalise socio-economically disadvantaged groups further." p. 2 last visited 18 June, 2020.

[166] Harvard Kennedy School: Evidence for Policy Design, available at https://epod.cid.harvard.edu/sites/default/files/2018-10/A_Tough_Call.pdf last visited (14-05-2020)

instead, as compared to only 16% men.[167] Most importantly, GSMA's Mobile Gender Gap Report, 2019 highlights how the gender gap typically widens for specific-use cases of internet-based mobile apps.[168] In a recent study conducted by the University of Oxford has closely studied the relationship between access to mobile phones and gender inequities.[169] Women without access to mobile phones are disproportionately impacted[170] by the transition to over-reliance on digital platforms instead of adopting traditional methods of communicating health information.[171]

> "Mobile phone use in personal healthcare is advantageous, already marginalized groups of individuals may be left out of healthcare access improvements, and they may face gradually growing exclusion from the health system"[172]

---

[167] *Id.*

[168]GSMA, The Mobile Gender Gap Report, available at https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/GSMA-The-Mobile-Gender-Gap-Report-2019.pdf (Last visited 14-05-2020); Giorgia Barboni, Erica Field, Rohini Pande, Natalia Rigol, Simone Schaner, Charity Troyer Moore, A Tough Call: Understanding barriers to and impacts of women's mobile phone adoption in India (October 2018), Harvard Kennedy School: Evidence for Policy Design, available at https://epod.cid.harvard.edu/sites/default/files/2018-10/A_Tough_Call.pdf last visited (14-05-2020); For a discussion on low smartphone access generally in India, see Divij Joshi & Amba Kak, India's digital response to COVID-19 risks inefficacy, exclusion and discrimination, https://caravanmagazine.in/health/india-digitial-response-covid-19-risks-inefficacy-exclusion-discrimination, (Last visited 14-05-2020). https://www.hindustantimes.com/world-news/indian-women-25-less-likely-to-own-mobile-phones-oxford/story-CJsgJzhvjzcdekB9g7nrMO.html.

[169]Prason Sonwalkar, Indian women 25% less likely to own mobile phones: Oxford, Hindustan Times, 9-06-2020, available at https://www.hindustantimes.com/world-news/indian-women-25-less-likely-to-own-mobile-phones-oxford/story-CJsgJzhvjzcdekB9g7nrMO.htm last visited 10 June, 2020.

[170]As already explained, a comprehensive review of the applicability of the disparate impact doctrine is beyond the scope of this Report. However, this discussion may be relevant while assessing the scale at which recommending the application may be suitable.

[171] *Id.*

[172]Haenssgen, M. J. "The Struggle for Digital Inclusion: Phones, Healthcare, and Marginalisation in Rural India." World Development, vol. 104, World Development, 2017, pp. 358–74. Several red zones identified by Aarogya Setu include slum areas as well. While some state governments have (albeit only since very recently) been proactive in supplementing digital contact tracing with door-to-door surveys (i.e. traditional contact tracing method, explained in detail under the necessity heading), there is very little publicly available information on the extent to which door-to-door surveys are taking place in every state, and if they are covering all the affected areas where smartphone-penetration is low; For an illustration of door-to-door surveys followed by identification of emerging hotspots, see https://www.hindustantimes.com/india-news/900k-people-241-zones-mumbai-s-mega-plan/story-19oqcbvvGRxnag7YdwzRFK.html.

Further, it is important to note that:

> "Even in contexts where mobile phones diffuse rapidly among individuals, households, and communities, people will continue to exhibit diverse arrangements for accessing mobile devices, which means that difficulties in utilizing the technology are likely to remain"[173]

Most importantly, the thesis concludes:

> "The gains from digital technology diffusion are deemed essential for international development, but they are also distributed unevenly. Does the uneven distribution mean that not everyone benefits from new technologies to the same extent, or do some people experience an absolute disadvantage during this process?...**inclusive innovation (in terms of mobile phone adoption) among parts of the poor population can...create new forms of exclusion elsewhere (potentially in terms of adverse socioeconomic impact). Indeed, during the process of diffusion, one may have to become digitally included to maintain the same relative position in healthcare access**"[174]

While few state governments have (albeit only recently)[175] been proactive in supplementing digital contact tracing with door-to-door surveys (i.e. a traditional contact tracing method) there is very little publicly available information on the extent to which door-to-door surveys are taking place in every state or context where predictions made by Aarogya Setu is a basis for further public health responses. It is not clear whether traditional contact tracing methods are covering all the affected areas where smartphone-penetration is low. Countries that are reporting the success of digital contact tracing are not able to attribute the success exclusively to digital contact tracing, divorced from other (including traditional) measures which facilitated the identification of symptomatic patients and hot spots, red-zones, et al. where risk-susceptibility is relatively higher.[176] Any such argument disregards and neglects other measures taken by governments to sustainably contain the spread of the virus.

---

[173]Haenssgen, M. J. "The Struggle for Digital Inclusion: Phones, Healthcare, and Marginalisation in Rural India." World Development, vol. 104, World Development, 2017, pp. 358–74.

[174]*Id.*

[175]Times of India, Covid-19 tests to be doubled in Delhi in next two days, door, 14-06-2020, available at Covid-19 tests to be ramped up; door-to-door survey in Delhi, last visited 18 June, 2020.

[176] *Id.*

Due to these reasons, the efficacy of digital contact tracing is not entirely certain; There is a **strong need for a periodic review of the assessment of the accuracy and effectiveness of the application**.[177] In the absence of sufficient evidence of proven efficacy, is it difficult to confirm with absolute certainty the suitability of digital contact tracing as a measure towards containing COVID-19. **Digital contact tracing should, therefore, at best only supplement and not *supplant* traditional forms of contact tracing and other appropriate health responses (including traditional contact tracing, enhancing abilities to conduct increased testing and isolating measures) as recommended by health experts**.

Even in situations where the application is used at present, **until further evidence verifying its efficacy is introduced, decisions such as ultimately zoning an indicatively emerging hotspot or decisions in terms of access of individuals should not be based wholly on the predictions made by the application**.[178] **The predictions made by the application should only serve an indicative purpose at best at this juncture**. **Any indication or prediction of the application should be verified with the help of other approaches including door-to-door surveys in emerging hotspots**. **This combined approach could help in making the application suitable for risk identification at the first instance**. **Risk identification at the first instance must be followed by subsequent steps towards confirming the risk by taking other measures** (e.g. door-to-door surveys in identified areas). Of course, false positives or negatives could continue to undermine the efficacy of the application; which is why the report re-emphasises the importance of verifying its efficacy with relevant evidence periodically in different contexts. However, this may reduce some short run costs by helping the government narrow down which areas to prioritise in addressing the Pandemic.

In order to promote digital contact tracing in the long run (i.e. beyond the six month period as indicated by the sunset clause discussed later), strong **evidentiary basis** of the efficacy of digital-contact tracing ***independent* of traditional methods** of contact tracing, and the statistical data on false positives and false negatives inferred from the application should be confirmed.[179]

To sum up: globally, four steps have been recommended as appropriate health responses to the Pandemic. These include testing, isolation, contact tracing, and finally isolating.[180] The

---

[177] *Id.*

[178] Rupsa Chakraborty, Such as, for instance, Door-to-door survey at heart of govt's Dharavi strategy to tackle Covid-19, Hindustan Times, 5-04-2020, available at https://www.hindustantimes.com/india-news/900k-people-241-zones-mumbai-s-mega-plan/story-19oqcbvvGRxnag7YdwzRFK.html last visited 18 June, 2020.

[179] *Id.*

[180] COVID-19: What Data is Necessary for Digital Proximity Tracing?, available at https://github.com/digitalepidemiologylab/COVID-documents/blob/master/COVID19%20Response%20-%

third step, i.e. contact tracing, could be done broadly in two ways: manually and digitally. Yet as explained above, the benefits of digital contact tracing are not evidenced at this juncture. Consequently, **it is critical to conduct a comprehensive review to identify the scale at which digital contact tracing is suitable in different demographic contexts in India** given particularly its socio-cultural diversity**.** The need for such a review would continue to remain since there still seems to be no publicly available information favouring the discontinuation of the Application any time soon. In fact, reports have suggested otherwise, i.e. that there is an intention to continue using the Application in the long run.[181]

The next section explains how measuring the extent of intrusion into privacy through Aarogya Setu against globally recognized best practices indicates that it is far more intrusive than is necessary to enable contact tracing.

Necessity

As stated above, (under the discussion on standard and intensity of judicial review), the necessity analysis involves looking at making two levels of comparison.

This section addresses the second level of comparison, i.e. Aarogya Setu with best international practices on digital contact tracing. As indicated in the suitability section, courts might, if adequate evidentiary basis is produced, conclude that the application satisfies the first comparison, (i.e. digital contact tracing is indeed indispensable given the pace at which it could be implemented). Again, this is subject entirely to the nature of evidence corroborating the suitability of the application before the court. On the second count, however, the court would have to assess whether Aarogya Setu as designed is minimally intrusive. Here, a review of **best international practices would have to be done[182] to determine the *extent* to which the Aarogya Setu is intrusive**. This requires an examination of:

1) Principally undermines **consent;**
2) The potential dangers of medical surveillance (i.e. 'privacy harms'). These **harms** can be best understood in the context of how consistent the application is with the international **best practices** on privacy safeguards, i.e. Fair Information Practice Principles ('FIPP').

20What%20Data%20Is%20Necessary%20For%20Digital%20Proximity%20Tracing.pdf last visited 10 June, 2020.

[181]Rhythma Kaul, Aarogya Setu gave forecasts regarding 650 Covid-19 clusters, 10-05-2020, available at last visited https://www.hindustantimes.com/india-news/aarogya-setu-alerted-about-650-clusters/story-1kvGonSkLz77dwH3zMYOQI.html last visited 14 June, 2020;("As such, it will be easier for individuals to find such hot spots to avoid further spread of the disease. In fact, this application will be more useful after the end of the lockdown," said Pradeep Awate, Maharashtra's state health surveillance officer.")

[182] *Id.*

Consent

The possibility of an obligation inter alia on employees to *mandatorily* use the application takes away the element of *choice* from the user, which is the essence of autonomy.[183] Generally speaking, decisional autonomy is one of the most crucial and quintessential aspects of the right to privacy.

In the context of the Pandemic specifically, it is not the mere absence of consent which is the problem: there is of course broad consensus towards containing the Pandemic. People may generally be willing to take steps towards participating in improving public health. This is particularly since the consequences of individual choices do not just affect the person's health but even others surrounding them. However, the problem is the absence of consent *combined* with the need to bolster transparency and privacy safeguards towards making the application conform to best practices internationally. People do not have any real choice in using Aarogya Setu (i.e. there is no less restrictive and widely accepted digital contact tracing method that is widely operationalized on a single platform).[184] This seems inconsistent with international best practices, as almost all countries have not made digital contact tracing mandatory.

Potential Harms (i.e. impact)

While the application seeks to conduct medical surveillance to adduce appropriate health responses, collection of information relating to professional status and real-time location data may cause a 'chilling effect'[185] on the freedom of speech. The most immediate effect could be illustrated: social activists or journalists (having to mandatorily use the application) may feel curtailed in reporting against the Government due to the fear of the government always knowing their precise location.[186] Further, since the information could potentially be shared with insurance companies for research, it could result in discriminatory consequences such as an increase in premium based on patient medical history picked up from the Application (the risk of specific patient identification continues to remain since the standard of anonymization is not clear from the privacy policy and the protocol).

[183] Press Information Bureau, Aarogya Setu is Now Open Source, available at last visited 27 May, 2020. https://pib.gov.in/PressReleasePage.aspx?PRID=1626979, last visited 27 May, 2020.
[184]2017 SCC 1.
[185] Shreya Singhal v. Union of India, (2013) 12 S.C.C. 73.
[186]Fatima Khan, Govt preventing Indian media from criticising it, reporting on pandemic: IPI, The Print, (16 May, 2020), available at https://theprint.in/india/govt-preventing-indian-media-from-criticising-it-reporting-on-pandemic-ipi/423095/ last visited (14-05-2020).

The Organisation of Economic Cooperation and Development ('OECD') outlined eight Fair Information Practice Principles of data protection which are conceptually like obligations on the entity processing the data of a user.[187] Evaluating the safeguards against these principles helps in understanding whether the Application in its present form constitutes the least intrusive method of realizing appropriate health responses. Below, seven of these principles (since the eighth principle relates to transnational transfers) to a conjunctive reading of the privacy policy and the protocol (these principles have not been discussed in order of priority and not their original order. So, the numbering might be different than what it ordinarily is):

Openness Principle

The Openness Principle necessitates that there is transparency and openness in practices and policies implemented to the user's data.[188] This means that the user should be able to find out the identity and residence of the data controller/fiduciary (i.e. the entity processing the individual's data). The privacy policy read with the protocol, even along with the source code (as already established above) however, does not create a framework for transparency.

The protocol does not recognize a right to explanation unlike the General Data Protection Regulation ('GDPR'), 2018, which in turn hurts openness further. The right to explanation could have entitled the user to inspect the algorithmic processes involved in making decisions concerning processing the user's data (e.g. at the GoI server, not the source code). The determination of what is an appropriate health response in a given situation may itself suffer from algorithmic bias. **Algorithmic bias could be of three types (i) input bias, (ii) training bias, and (iii) programming bias. Input bias occurs when the algorithm is fed inadequate information of a certain type or parameter**.[189] Given that women have relatively very low access to the internet and particularly to smartphones (which are Aarogya Setu-enabled)[190] the algorithmic model governing the GoI server may make faulty

[187]Organization of Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Last visited 14-05-2020).

[188]*Id.*

[189] Karen Hao, This is how AI bias really happens—and why it's so hard to fix, MIT Technology Review, (February 4, 2019), available a thttps://www.technologyreview.com/2019/02/04/137602/this-is-how-ai-bias-really-happensand-why-its-so-hard-to-fix/, (Last visited 14-05-2020).

[190]GSMA, The Mobile Gender Gap Report, available at https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/GSMA-The-Mobile-Gender-Gap-Report-2019.pdf (Last visited 14-05-2020); Giorgia Barboni, Erica Field, Rohini Pande, Natalia Rigol, Simone Schaner, Charity Troyer Moore, A Tough Call: Understanding barriers to and impacts of women's mobile phone adoption in India (October 2018), Harvard Kennedy School: Evidence for Policy Design, available at https://epod.cid.harvard.edu/sites/default/files/2018-10/A_Tough_Call.pdf last visited (14-05-2020); For a discussion on low smartphone access generally in India, see Divij Joshi & Amba

assumptions or judgments on the likelihood of a female user contracting COVID-19 based on their data. Training bias occurs when the source code incorrectly categorizes the input data. Programming bias occurs when the original design is allowed to be modified by successive interaction with human uses, which could itself create a further bias (e.g. a user providing incorrect information relating to any parameter (e.g. age) to the Application which the Application cannot verify).[191]

The protocol imposes an obligation on the NIC to explicitly state the Response data and the purposes for which the information is collected by the NIC. This seems to be a limited obligation to notify the user through the privacy policy of the:

a) types of information that are being collected as response data and
b) the purposes for which it is collected.

However, there is no clear obligation to provide explicit notice regarding such information or privacy policy to the user. Most users perhaps disregard the privacy policy at the time of downloading the application. The privacy policy of the Application is quite difficult to locate on the interface from which the Application is downloaded. While at present, users need to use the application irrespective of whether or not they are willing to do so, principles of fairness necessitate that users receive explicit notice about the type of information that is being processed and the purposes for which it is collected. This is because, unless users have a right to be aware of associated risks with using Aarogya Setu, they would not even be making an *informed* decision when they download and use the Application (particularly in cases where an active choice is made to use the Application in the absence of any mandate). As explained under the section explaining why aarogya Setu is still mandatory, why openness and transparency are critical is discussed in more detail.

The Data Quality Principle

The Data Quality Principle requires that only such personal data is collected as is relevant to achieve a particular purpose, in this case, for appropriate health responses.[192] The Application collects information relating to the '**professional status'** of the user (i.e. whether the user is a lawyer, journalist, activist, student, etc.). It is not clear as to why *professional*

Kak, India's digital response to COVID-19 risks inefficacy, exclusion and discrimination, https://caravanmagazine.in/health/india-digitial-response-covid-19-risks-inefficacy-exclusion-discrimination, (Last visited 14-05-2020).

[191]Nizan Geslevich Packin, Yafit Lev-Aretz, *Learning algorithms and discriminations*, RESEARCH HANDBOOK ON THE LAW OF ARTIFICIAL INTELLIGENCE, p. 96.

[192]Organization of Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Last visited 14-05-2020).

status is information relevant for appropriate health responses. The necessary link between a health response to the profession of the individual is not clear. The app in any case collects the real-time location information of the user which makes it possible to trace the people with whom the user may have come in contact. Additionally, collecting information relating to professional status seems inconsistent with the data quality principle.

Collection Limitation Principle

The collection limitation principle protects users against aggregation of more information about them than is necessary to achieve a purpose.[193] The protocol precludes the NIC from collecting more response data than is necessary and proportionate to implement or formulate appropriate health responses to contain COVID-19. The protocol also necessitates that the extent of personal data collected must be strictly proportionate to the objective of realizing appropriate health responses. Assuming only such information is being processed as is stated in the protocol and therefore with the knowledge or consent of the user, the protocol is consistent with the collection limitation principle.

Inadequate Obligations against Disclosure

Since the Application collects not only location information but even *health* data in evaluating whether a user is symptomatic or not, any disclosure to third parties can subject the user to harms such as stigmatization[194] which could translate into sorting (i.e. labelling them into stigmatic categories such as someone with COVID-19 for the rest of their lives which is of course not inherently problematic apart from the stigma), discrimination (i.e. denial of insurability or increase in insurance premium based on pre-existing medical condition, i.e. history of. COVID-19) or extortion (i.e. someone gaining unauthorized access to personal or sensitive personal data uploaded on the Application to make an unlawful gain or cause a user undue loss, monetary, reputational, personal or otherwise).

Given the possibility of these harms, the obligations imposed on the NIC against disclosure to third parties constitute one of the most important parts of the discussion. The protocol enables the NIC to share the response data collected with the Health Ministry, state health departments, state, Union Territory and local governments respectively, National Disaster Management Authority, state disaster management authority and other public health institutions of the local, state and central governments provided that the "sharing is strictly necessary to directly formulate or implement an appropriate health response."[195]

---

[193] *Id.*

[194] Ministry of Health and Family Welfare, Circular, Addressing Social Stigma Associated with COVID-19, available at https://www.mohfw.gov.in/pdf/AddressingSocialStigmaAssociatedwithCOVID19.pdf (Last visited 14-05-2020).

[195] Vidhi Centre for Legal Policy, *Aarogya Setu's Data Access and Knowledge Sharing Protocol*, (May 09, 2020), available at

However, **such sharing is not subject to a corresponding requirement that the NIC share only such extent of information as is strictly proportionate to attain the appropriate health response**. Therefore, the obligation against disclosure is inconsistent with the collection limitation principle. It is not clear why the obligation against disclosure is not subject to an obligation to share only such information as is proportionately required. If the obligation to share information proportionately were present, it would ensure that only a minimum extent of information is disclosed towards formulating an appropriate health response.

Additionally, **there is also no obligation to notify users when their information is disclosed to a third party about the type of information shared and the identity of the entity with which the information is shared**. Neil Richards has explained how secret surveillance is dangerous and undesirable. Medical surveillance must be transparent about the entities which are responsible for processing user data.[196]

The protocol further enables the sharing of response data with Indian Universities, Research institutions, and research entities registered in India. Both '**Research Institutions' and 'Research Entities' are not defined in the protocol**. It is not clear whether the meaning of research institutions is restricted to organizations (e.g. think-tanks) involved exclusively in medical research, **or whether even research and development units of industries would have access to such information**. For example, insurance industries themselves are perhaps engaged in conducting research relating to the predictive analytics to understand the average life-span of a person with a history of COVID-19 along with some other condition (e.g. life expectancy based on travel records (e.g. due to inevitably unsafe route to travel to work), past medical history, presence of symptoms, etc).[197] **It is not clear whether research entities or institutions encompass functioning research units that operate independently but are structurally integral to existing industries in the private sector**. As already established, **sharing medical data opaquely with private entities can exacerbate privacy harms such as discrimination through surveillance capitalism** (e.g. discriminatory insurance premiums between two different users, when one user is more susceptible to health risks).[198] The clause which allows for the sharing of this information for research is not qualified with the requirement that the research should endeavor to attain public good as opposed to meeting

---

https://vidhilegalpolicy.in/2020/05/11/aarogya-setus-data-access-and-knowledge-sharing-protocol-2020/ (Last visited 14-05-2020).

[196]Neil Richards, *The Dangers of Surveillance*, Harvard Law Review 126 (1934) (2012)

[197]Binayak Dasgupta, Protection or threat? Experts say Aarogya Setu poses national security risk, Hindustan Times (23 May, 2020), available at https://www.hindustantimes.com/india-news/aarogya-setu-protection-or-threat/story-QmpSP3H60ohkLV3l5ywhBI.html, (last visited 29-05-2020); Arya Tripathi, Are insurtech users compromising on their data privacy for convenience?, Mint available at https://www.livemint.com/insurance/news/are-insurtech-users-compromising-on-their-data-privacy-for-convenience-1563357891706.html (last visited 29-05-2020).

[198] SHOSHANA ZUBOFF, SURVEILLANCE CAPITALISM, 2018.

with private interests. Of course, the distinction itself may be difficult to draw in several cases.[199]

The Individual Participation Principle

The principle of individual participation entitles an individual with the right to confirmation of whether or not the data fiduciary has information that relates to such a user.[200] At present, both the privacy policy and the protocol are bereft of a right to confirmation, which makes it impossible for an individual to inquire into whether NIC or any other government agency continues to retain user information collected by the Application after the expiry of the sunset clause (which is discussed later in the paper).

The Accountability Principle

The principle of accountability requires that data fiduciaries are held accountable for failing to comply with the other fair information protection principles.[201] The protocol refers to accountability but does not create any penal provisions for failing to comply. It might be important to look at the extent to which the NIC operates independently of the Government of India in terms of control and supervision to attribute any responsibility to either entity for harms that may arise (vicariously or otherwise) as a result of such processing.

It is also important to note that since the protocol was published as a Government Order independent of the framework under the NDMA, any failure to comply may not be a violation of the NDMA. Therefore, for data breaches, the Government may not be responsible under any residuary penal provision. Therefore, the protocol does not adequately incorporate the principle of accountability. At best, the incorporation of the principle is vague and toothless.

---

[199]See Chaoulli v. Quebec, (AG) [2005] 1 S.C.R. 791, where the Supreme Court of Canada struck down a restriction against private participation in the insurance sector in Canada due to the inability of the public sector to meet with the public health needs of every person. The prohibition was introduced with the assumption that private sector participation could undermine public good since it would result in rise in premium and insurance-related costs and also result in shrinking the public insurance pool. The majority opinion which felt that private sector participation could benefit the public highlights that drawing a distinction between public good and private good may be very murky.

[200]Organization of Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Last visited 14-05-2020).

[201]Organization of Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Last visited 14-05-2020).

The Purpose Specification Principle

The purpose specification principle necessitates that *at the time of collection* of personal data, the user is notified what is the purpose of collection. The privacy policy specifies the purpose of the Application as follows:

> "The personal information collected from you at the time of registration under Clause 1(a) above, will be stored on the Server and only be used by the Government of India in anonymized, aggregated datasets **to generate reports, heat maps and other statistical visualizations for the management of COVID-19 in the country or to provide you general notifications about COVID-19 as may be required**"

The Protocol further specifies the purpose in the following words:

> "such data shall be used strictly to formulate or implement appropriate health responses and constantly improving such responses."[202]

There seems to be considerable overlap between the two, i.e. the purpose of the collection broadly seems to be to develop appropriate health responses to contain COVID-19. Therefore, one could argue that the privacy policy read with the Protocol is consistent with the purpose specification.

The Security Safeguards Principle

The security safeguards principle requires that the entity processing personal data undertake and implement reasonable security safeguards to mitigate risks or harms to users, such as unauthorized access, use, destruction, modification, or disclosure of data to third parties.

[202] Aarogya Setu Application, Data Access and Knowledge Sharing Protocol, 2020, available at https://meity.gov.in/writereaddata/files/Aarogya_Setu_data_access_knowledge_Protocol.pdf (Last visited 14-05-2020).

Privacy-conscious digital contact tracing encouraged globally necessitates that the data stored through the Application is decentralized.[203] At the same time, decentralization has the potential of undermining the usefulness of the health data.[204]

Arogya Setu, on the other hand, centralizes all the data in the GoI server, the working of which indicated above, continues to remain a black box.

Overbroad Data Retention (Sunset) Clause

The protocol necessitates the NIC to permanently delete a location, contact, and self-assessment data after 180 days under ordinary circumstances.[205] However, the protocol does not specify under what circumstances may such data be retained for longer (i.e. what constitutes an *extraordinary* circumstance warranting retention of data beyond 180 days). A recommendation to retain the data for longer would trigger further retention of such data. The *basis* on which the Empowered Group constituted by the MeitY could further recommend the NIC to continue retaining the data is not clearly stated in the Policy.

Further, demographic data of an individual is to be retained for as long as the protocol remains in force or within thirty days since whenever the individual seeks to exercise their right to delete such data, whichever date comes earlier. It is not clear until when will the protocol remain in force at this juncture, given that the future of COVID-19 also remains uncertain.

Cumulatively examining these concerns suggests that there is further scope to make the governing framework of the application (i.e. the privacy policy and the protocol) more robust and significantly less intrusive in order to satisfy the necessity prong. Next, the balancing of privacy and public health is done. To sum up, given the sensitive nature of the data which is being collected (i.e. demographic data, location data, data about symptoms, etc), applying the standard of reasonableness in reviewing the constitutionality of the Application may not be appropriate. Instead, whether the governing framework of the application is designed in the least restrictive manner should be examined, as this would contextually do greater

[203]Joe Duball, International Association of Privacy Professionals, Centralized vs. decentralized: EU's contact tracing privacy conundrum, available at https://iapp.org/news/a/centralized-vs-decentralized-eus-contact-tracing-privacy-conundrum/ last visited 10 June, 2020.

[204] Jen Patja Howell, The Lawfare Podcast: Is Contact Tracing a Privacy Threat? Lawfare, available at http://www.lawfareblog.com/lawfare-podcast-contact-tracing-privacy-threat last visited 10 June, 2020.

[205]Aarogya Setu Application, Data Access and Knowledge Sharing Protocol, 2020, available at https://meity.gov.in/writereaddata/files/Aarogya_Setu_data_access_knowledge_Protocol.pdf (Last visited 14-05-2020).

justice to alleviating concerns regarding the privacy harms that could arise out of using the application. Therefore, the standard of judicial review which should be assessed is whether Aarogya Setu is the least restrictive intrusion into privacy. The burden to prove that the least intrusive method of achieving appropriate health responses has been met with should lie with the Government of India.

The Balancing Stage

The proportionality prong of the test broadly requires an evaluation of the benefit of the mandate to use Aarogya Setu against the harms that it can potentially cause to the right to privacy.[206] In essence, the intrusion (i.e. the mandate to use the Application) has to be balanced with the compelling public interest (i.e. public health-related interest in containing COVID-19) so that the intrusion is not disproportionate.

There is, of course, a compelling public interest in ensuring that the pandemic is contained. However, it is not clear whether using Aarogya Setu instead of undertaking alternative measures is the least intrusive way of predicting appropriate health responses. As established earlier, there are less intrusive ways to contain the virus than digital contact tracing, including increased testing, traditional methods of contact tracing, and the process of isolating potential cases. These methods are not only less intrusive but are also consistently proven to be effective ways to combat COVID-19. Even if one is to concede and assume the efficacy of digital contact tracing for a moment, it is seen from above that the Application is inconsistent with the Fair Information Protection Principles.

While balancing privacy and public health, it becomes crucial to recognize that both these interests do not necessarily conflict with each other.[207] Privacy and public health are *complementary* values, each strengthening the other.

Amartya Sen recently wrote, 'listening' during the pandemic is crucial to address public health concerns.[208] Sen's articulation aimed at highlighting the importance of strengthening

[206]Bilchitz, David, Necessity and Proportionality: Towards a Balanced Approach? (August 17, 2012). Reasoning Rights (Edited by L. Lazarus, C. McCrudden and N. Bowles) (Hart, 2014, Forthcoming). Available at SSRN: https://ssrn.com/abstract=2320437 last visited 10 June, 2020.

[207]Rahul Matthan, Liberties Yielded in this Crisis Set the New Normal, Mint, (Mar 25, 2020) available at https://www.livemint.com/opinion/columns/liberties-yielded-in-this-crisis-could-set-a-new-normal-1158507 3864193.html, last visited (14-05-2020); Yuval Harari, Financial Times, *The World after CoronaVirus* (Mar 20, 2020), available at https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75 (Last visited 13-05-2020).

[208]Amartya Sen, Indian Express, *Amartya Sen writes: Overcoming a pandemic may look like fighting a war, but the real need is far from that* (Apr 08, 2020), available at

democratic institutions so that governments are more accountable for failing to address concerns emerging from the pandemic. To illuminate this argument, Sen refers to his earlier work, *Development as Freedom*[209], where he explained how the greatest number of public health disasters occurred in erstwhile colonies, where civil liberties of people were greatly undermined. Democratic institutions, therefore, need to be particularly strong during the pandemic as in their absence, there is no way to highlight the failure of the government in tackling different issues arising from the pandemic.[210]

In several states, the Press, for instance, has played a significant role in highlighting the failures of the government in doing adequate testing for detection of COVID-19, procuring masks and other protective equipment, and providing adequate social security during the lockdown to the most vulnerable groups. Civil liberties such as privacy are instrumental towards ensuring Freedom of the Press during the pandemic.[211] It is a settled position that privacy *inter alia* serves as an instrument to ensure related civil liberties such as the freedom of speech.[212] The importance of civil liberties during the pandemic highlights that there is no real dichotomy between privacy and public health. This balancing needs to be done keeping in mind the conception of the relationship between privacy and public health as complementary to each other.

Based on the complementary nature of these two values, the balance should not be predisposed to view the pandemic as an extraordinary circumstance which warrants that principles of proportionality are entirely disregarded so that extraordinary measures, as Kerala High Court problematically points out, are taken.[213] The fact that we are undergoing a pandemic is only relevant to underscore the *necessity* of a particular restriction so that the balance tilts slightly in its favor. However, the proportionality analysis would still require that the manner and conditions of imposing the mandate should *still* be least restrictive. As already indicated, the Application is not adequately consistent with all the Fair Information Protection Principles ('FIPP'). Therefore, the Application is yet to satisfy the standard of being

---

https://indianexpress.com/article/opinion/columns/coronavirus-india-lockdown-amartya-sen-economy-migrants-6352132/ (Last visited 14-05-2020).

[209]Amartya Sen, Development as Freedom, 1999.

[210]Rahul Matthan, Liberties Yielded in this Crisis Set the New Normal, Mint, (Mar 25, 2020) available at https://www.livemint.com/opinion/columns/liberties-yielded-in-this-crisis-could-set-a-new-normal-1158507 3864193.html, last visited (14-05-2020);

Yuval Harari, Financial Times, *The World after CoronaVirus* (Mar 20, 2020), available at https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75 (Last visited 13-05-2020).

[211]Amartya Sen, Development as Freedom, 1991.

[212]Justice KS Puttaswamy & Ors. v. Union of India & Anr. (2017) 10 SCC 1.

[213]Bar and Bench, *"Extraordinary situations call for extraordinary measures" Kerala HC adjourns plea against mandatory imposition of Aarogya Setu to May 18* (May 12, 2020), available at https://www.barandbench.com/news/litigation/extraordinary-situations-call-for-extraordinary-measures-kerala-hc-adjourns-plea-against-mandatory-imposition-of-aarogya-setu-to-may-18 (Last visited 14-05-2020).

the least restrictive way of attaining appropriate health responses to COVID-19. It is hoped that more positive steps are taken towards ensuring its consistency with the FIPP.

RECOMMENDATIONS

Over and above the steps already taken towards transparency along with publicising the manner of processing at the server code soon, the following could be one towards further bolstering privacy and other safeguards:

1. Further steps towards increasing transparency in the operability of Aarogya Setu are welcome. This would ensure that it is possible to identify potential algorithmic biases and *enable* the mitigation of some harm.This could be done by releasing further information on the parameters or the guiding principles behind the predictions made by the GoI server to the public. This would make the algorithm guiding the decision-making meaningfully transparent. A right of users to a comprehensive explanation as to how their information is being processed could be an example of a step geared towards meaningful transparency. **However, transparency is only a means to identify privacy harms, paving the way for appropriate privacy safeguards;**
2. The sunset clause should have a hard deadline of six months, after which a new legislative process should reincarnate the legal basis to use the application. This would help in strengthening the characterisation of the duration for which the data may be exposed as transient instead of permanent;
3. Information on the standard of anonymization to which the information collected by the Application should be specified or a general idea of the same should be outlined in the protocol itself. This would ensure that there is some degree of notice if there is any change in the standard. This would also alleviate cybersecurity concerns that are raised by the possibility of reidentification of user data;
4. A robust framework of accountability and a notification in case of breach of information collected by the Application to the user should be created. This would ensure that individuals are both aware of situations where their rights have been compromised and can take steps towards mitigating associated harms;
5. The Application could be made meaningfully voluntary through public advisories which explicitly mention that using the Application is not mandatory. Further, there should be some recourse available if a private party (e.g. an employer) makes the Application mandatory;
6. Sharing of information, in the interests of privacy, could be limited strictly to public health departments only since the information is strictly necessary for appropriate health responses;
7. The definition of a research institution should be clarified and restricted to only non-profit organizations. This would ensure that health data is not potentially misused for monetization by entities in the private sector;

8. Traditional methods of contact tracing (e.g. door-to-door surveys) should be stepped up to verify the predictions of the Application, to ensure that digital contact tracing does not entirely replace traditional methods

9. Periodic review of the efficacy of the application could be publicized to bolster faith in the system and alleviate concerns of false positives or negatives that could potentially arise from a digital contact tracing architecture

10. **The Personal Data Protection Bill (PDPB'), 2019[214] yet to come into force does not categorize *location* data as 'sensitive personal data'**. As indicated in inter alia *Carpenter,* however, location data over time can reveal a lot more about an individual, if viewed cumulatively, than an individual would ordinarily imagine.[215] The definition of sensitive personal data under the Bill currently does not include location data. Location data, as already established, can unintentionally reveal extremely intimate facts about an individual, which could expose them to significant privacy harms that are comparable in terms of gravity to the harms caused by exposure of other types of sensitive personal data.[216]

    It is therefore clear that in reality there exists no hierarchization between sensitive personal data and location data in terms of gravity (since the exposure of location data to vulnerabilities can be very harmful to the user). Therefore, the definition of sensitive personal data should include location data (collected over a sustained period).

    The benefit of categorizing location data as sensitive personal data is that once a data protection framework comes into being, assuming digital contact tracing continues to take place (which is quite likely)[217], it precludes government agencies from being exempt from obligations towards such data. Under the proviso to section 35[218], in the interests of national security or maintenance of public order, the Central Government could exempt any government agency from provision relating to the processing of *personal data*.

    A strict reading of the exemption provision suggests that it does not exempt government agencies from obligations concerning *sensitive* personal data. Since the phrase sensitive personal data has been separately and explicitly defined under the

[214] Personal Data Protection Bill, 2019.
[215] Carpenter v. United States, No. 16-402, 585 U.S. (2018).
[216] Neil Richards, *The Dangers of Surveillance*, Harvard Law Review 126 (1934) (2012).
[217]Rahul Matthan, Liberties Yielded in this Crisis Set the New Normal, Mint, (Mar 25, 2020) available at https://www.livemint.com/opinion/columns/liberties-yielded-in-this-crisis-could-set-a-new-normal-1158507 3864193.html, last visited (14-05-2020).
Yuval Harari, Financial Times, *The World after CoronaVirus* (Mar 20, 2020), available at https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75 (Last visited 13-05-2020).
[218] Personal Data Protection Bill, 2019, §35.

Bill, assuming that any reference to personal data per se is also a reference to sensitive personal data may be an unfair assumption to make. Therefore, one could argue that sensitive personal data enjoys greater protection insofar as inter alia exemptions to government agencies are concerned. Therefore, it may be of value for the Joint Parliamentary Committee on the Personal Data Protection Bill, 2019 ('**JPCPDPB**') to consider an amendment to the Bill to include location data as a subcategory of sensitive personal data under the Bill. This would ensure that government agencies cannot be exempt from the applicability of all the data protection obligations under the Bill, assuming it is enacted anytime soon (during the period in which the response data continues to be retained by government agencies).

CONCLUSION

To sum up, the information collected when using Aarogya Setu includes sensitive personal data and personal data, over which an individual exercises a reasonable expectation of privacy. The recommendation to use Aarogya Setu is a de facto mandate that imposes some limitations on privacy. This, in turn, could, in the absence of adequate safeguards, potentially lead to harm such as a rise in premium costs in insurance policies hurting vulnerable groups the most, making them more susceptible to sorting (i.e. healthy or not based on non-transparent parameters), profiling, or discrimination (e.g. exclusion from insurance coverage). The safeguards present in the privacy policy and the protocol collectively can be increased towards greater conformity with international best practices to make it the least intrusive alternative. Further, limitations imposed on privacy need to be proportionate to the need to formulate appropriate health responses during the Pandemic. Based on the existing legal position on the meaning of 'law', the combined reading of the general enabling provision under the NDMA and the G.O indirectly mandating the use of Aarogya Setu may satisfy the first prong of the test, i.e. lawfulness. Containing the pandemic is also of course a legitimate object. However, it is suggested that Parliamentary legislation is nevertheless introduced to govern the operability of the application in the long run to ensure greater predictability and accountability in imposing compromises on privacy in the interests of public health

Further, the change in the mandate from a 'must' to a 'should' in the G.O is welcome; however, the same should be communicated better through advisories explicitly mentioning that using the Application is not mandatory so that the general public can make informed choices. The recommendations suggested above are *only* an indicative list of how improvements could be made. These efforts could help in ensuring that the Application is more consistent with best international practices on digital contact tracing. Ameliorating concerns of effectiveness, transparency, and privacy could infuse further credibility into the program, creating a stronger incentive to use Aarogya Setu, towards greater effectiveness.