scripted

Volume 20, Issue 1, February 2023

Operationalizing Privacy by Design: An Indian Illustration

*Ankit Kapoor**

DOI: 10.2966/scrip.200123.5

Abstract

This article identifies Privacy by Design ["PbD"] as a suitable regulatory approach to address the attack on personal data in the Fourth Industrial Revolution. It proposes Privacy Engineering ["PE"] as a concrete methodology to operationalize the otherwise vague Privacy by Design. Privacy Engineering operationalizes the normative knowledge of privacy into specific use cases through layers of flexible abstract thinking, interconnected through a "web of templates". This "web of templates" can be constructed by answering the two-fold question of relevancy and extent of data protection required. PE provides regulators with a specific language in which they can communicate with data controllers to establish privacy obligations and undertake prioritized capacity building for resource-deprived data controllers.

This article also illustrates the application of this methodology through the Account Aggregator Framework and the Aarogya Setu Application. Positioning this method as not just an operational guide but also a rigorous tool of critique, it also evaluates the extent of their compliance. Account

Aggregator exceptionally embodies PbD, while Aarogya Setu does so only averagely.

Keywords
Personal Data Protection; privacy by design; privacy engineering; Aarogya Setu application; account aggregator framework

* 5th Year Student, B.A.-L.L.B, National Law School of India University, Bangalore, India, ankitkapoor@nls.ac.in. The author would like to thank Mr. Rahul Matthan for his inputs and his enlightening seminar course.

1 Introduction

The Fourth Industrial Revolution, characterized by unprecedented global convergence of digital, physical, and biological technologies, is rapidly changing the inherent value and usability of data. As new and current technologies go digital, the amount of data processing is increasing, with its frequency almost surveillance-like. Even the manner of data processing is expanding from merely active to also passive forms. Digital interoperability has generated large databases from otherwise isolated and meaningless information. Coupled with algorithmic ingenuity in successful predictions, it is now possible to know more from less.

Data is the primary unit to analyze behavior, identify preferences, and thereby efficiently target commodity delivery. This growing incentive in usage indicates that data is truly the new oil. Moreover, the intangibility and reusability of data has enabled its infinite global distribution. These changes can collectively be termed as 'the paradigm shift of the Fourth Industrial Revolution'. Given this paradigm shift, traditional forms of regulation are ineffective. Failure to tackle this attack on privacy will not only mitigate the revolutionary potential of these technologies, but also compound power imbalances and global inequalities. Considering this, novel regulatory approaches need to be adopted.

Accordingly, in this paper, I analyze the inadequacies of the 'consent framework' to address the paradigm shift of the Fourth Industrial Revolution. As an alternative, I identify the concept of "Privacy by Design" ("PbD") as an effective regulatory approach in this age, and justify policy intervention in technological design. Subsequently, addressing PbD's vagueness and non-implementation critique, I declutter the "Privacy Engineering" ("PE") methodology, and explain how it better operationalizes PbD through an "interconnected web". I also explain the utility of this method and its manner of

incorporation within regulatory frameworks. Ultimately, I critically analyze the Account Aggregator Framework and the Aarogya Setu Application through the lenses of this modified PbD methodology. Through this, I demonstrate the application of this PE methodology in a specific use case. Additionally, I illustrate the extent of compliance by these two technologies, and suggest improvements, wherever necessary.

This paper makes three unique contributions to existing literature: (1) it clarifies the confusion on the nature of and relationship between different elements of the PE methodology; (2) it provides a specific regulatory approach to deploying PE in any data protection legislation, and demonstrates its utility; (3) against a background of scant PbD literature in India, it applies and evaluates PE in the context of two contemporary and headline-generating Indian technological solutions: the Account Aggregator Framework and the Aarogya Setu Application.

2 Inadequacy of current legal framework

Globally, the bedrock of the current data protection framework is notice and consent. Once notice of data processing is provided to the data subject, and consent is obtained thereof, the data controller is free to utilize such data for the specified purpose without any ensuing consequences.[1] Therefore, the burden is on the data subject to carefully and meaningfully provide consent. However, the 4th Industrial Revolution's paradigm shift, as illustrated above, renders the consent mechanism futile, by itself.

[1] Rahul Matthan, 'Beyond Consent – A New Paradigm for Data Protection' (2017) Takshashila Discussion Document 3/2017, 2-3 <https://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf> accessed 16 October 2020.

The purposes of data collection are, contractually, phrased broad and vague enough to extend their application to future events, which users never foresaw.[2] The volume and frequency of data collection undertaken through technical and voluminous standard form contracts, coupled with the number of such contracts concluded, leads to a "consent fatigue" among data subjects. Thus, it is unfeasible to expect extensive knowledge of contractual terms from the data subject.[3] Moreover, the interoperability of modern databases allows interaction of distinct datasets to produce unique and powerful insights. Typically, privacy policies extend consent to such data interactions. Since it is implausible to pre-determine these unpredictable insights, consent to such collection is naturally uninformed.[4]

Machine learning algorithms are so good at spotting patterns and profiling that even data that an individual did not consent to sharing can be obtained using smaller samples of consensually shared data along with other databases containing some information on this individual.[5] The complexity of modern privacy policies creates uncertainty among data subjects and controllers regarding the standard of data protection. This uncertainty is itself costly, as it forces consumers and firms to invest resources into learning about the

---

2 Joel Reidenberg, Jaspreet Bhatia, Travis Breaux and Thomas Norton, 'Ambiguity in Privacy Policies and the Impact of Regulation' (2016) 45(2) JLS <https://www.journals.uchicago.edu/doi/abs/10.1086/688669?journalCode=jls> accessed 16 October 2020.

3 Matthan (n 1); Joel Reidenberg, Stanley D, et al, 'Privacy Harms and the Effectiveness of Notice and Choice Consent Framework' (2014) 11(2) Journal of Law and Policy for the Information Society 485, 490-496.

4 Ibid.

5 Ibid.

acceptability of a particular data practice.[6] Subsequently, this pushes consumers and firms to, depending on the context, invest sub-optimally in data protection.[7]

Thus, the consent model disproportionately and untenably holds the data subject accountable for data protection.

The problem compounds because the consent model is excessively over reliant on *post facto* rights-based litigation. It is difficult to establish concrete basis for violations as there is seldom transparent access to means of verifying the actual implementation of the purposes for which consent was obtained. While there are legal means to compel access, their drawn-out and expensive nature disincentivizes engagement. Even where data subjects can prove that data was processed without consent, the consequent monetary compensation is inadequate when factoring the overall cost of the process. Moreover, monetary sums need not be sufficiently remedial in various circumstances. Anyhow, the approach embodied herein does not consciously seek to prevent harms.

3 Intervention through Technological Design

Evidently, due to advancements in emerging technologies, there is a need to look beyond consent to effectively regulate data protection. Accordingly, I argue for adopting a design thinking perspective, where risks are anticipated and countermeasures are baked into the systems and operations throughout the lifecycle of the system/product/process.[8] Notably, PbD recognizes that while consent is necessary, it is by no means sufficient.

---

6 Alessandro Acquisti, 'The Economics of Personal Data and the Economics of Privacy' (2010) OECD Background Paper 3/2010, 13-14 <https://www.oecd.org/sti/ieconomy/46968784.pdf> accessed 16 October 2020.

7 Ibid.

8 Ann Cavoukian, 'Privacy by Design: The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices' (*Information and Privacy Commissioner*, 2011) <https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf> accessed 22 September 2020.

3.1 Adopting Privacy by Design

PbD is an approach to systems engineering based on proactively embedding privacy into the design and operation of networked data systems and technologies as well as organizational practices.[9] It was the brainchild of Dr. Ann Cavoukian, introduced in the 1990s. Since then, it has received overwhelming support not only at various data protection conferences, but more importantly in privacy legislations of various countries.[10] In most jurisdictions, it remains a voluntary industry obligation, with minimal regulatory promotion.[11] However, in some jurisdictions, like the European Union and soon India, it is a binding obligation on all data controllers. Nevertheless, the nature and extent of this binding obligation varies.

The biggest difference between the two is when compliance must be demonstrated. In India, the approval process must happen before the data controller officially commences data processing.[12] However, in the EU, data controllers can choose to undergo certification, in which case this serves as proof of compliance,[13] or can simply demonstrate compliance when violation is alleged against them.[14]

---

9 Ibid.

10 European Union Agency for Network and Information Security (ENISA), 'Privacy and Data Protection by Design – from policy to engineering' (2014), 1-5 <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design> accessed 22 January 2023.

11 Ann Cavoukian, 'Privacy by Design in Law, Practice and Policy: A White Paper for Regulators, Decision-makers and Policy-makers' (*Information and Privacy Commissioner*, 2011) <http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf> accessed 16 October 2020.

12 Data Protection Bill 2021, s 22(1)-2(2).

13 General Data Protection Regulation 2018, art 42.

14 General Data Protection Regulation 2018, art 25(1).

3.2 The Seven Foundational Principles and their corresponding FIPs

The seven foundational principles of PbD provide guidance on applying the design thinking perspective. They not only seek to operationalize globally accepted Fair Information Practices ("FIPs"), but also extend beyond them. This is particularly important since these FIPs have been adopted within domestic legislations, globally. For instance, the General Data Protection Regulation ("GDPR") and Data Protection Bill, 2021 ("DPB") require the data to be processed with lawfulness, fairness and transparency,[15] for the purpose to be specific, explicit and limited,[16] adequate, relevant and necessary to required purpose,[17] accurate,[18] stored only for the period necessary,[19] and secure.[20]

Against this background, it is useful to understand the seven foundation principles. They are:[21]

(1) Proactive not Reactive; Preventative not Remedial: This approach is based on anticipating and preventing privacy invasions in an *ex ante* manner.

(2) Privacy as the Default**:** Regardless of any intervention by the data subject, every system should be engineered to automatically protect privacy, by default. These FIPs guide this default setting:

- *Purpose Specification*: The purposes for processing data should be clear, limited, relevant to functions, and specified to the user prior to processing.
- *Collection Limitation*: The data must be collected in a manner that is fair, lawful, and limited to specified purpose.

---

15 General Data Protection Regulation 2018, art 5(1)(a); Data Protection Bill 2021, s 4-5.
16 General Data Protection Regulation 2018, art 5(1)(b); Data Protection Bill 2021, s 5.
17 General Data Protection Regulation 2018, art 5(1)(c); Data Protection Bill 2021, s 6.
18 General Data Protection Regulation 2018, art 5(1)(d); Data Protection Bill 2021, s 8.
19 General Data Protection Regulation 2018, art 5(1)(e); Data Protection Bill 2021, s 9.
20 General Data Protection Regulation 2018, art 5(1)(f).
21 Cavoukian (n 8).

- *Data Minimization*: The identifiability, linkability, and observability of personal data must be at a strict minimum.
- *Use, Retention, and Disclosure Limitation*: These must be limited to the specified purposes consented to. Moreover, data should be retained only for the necessary period, thereafter, being destroyed.

(3) Privacy Embedded into Design**:** Privacy must be embedded into the architecture and design of IT systems and organizational practices. In doing so, existing choices are re-invented to render privacy as a core functionality of the process.

(4) Full Functionality – Positive-Sum, not Zero-Sum**:** Through re-engineering, PbD accommodates all legitimate interests, thus evading the traditional dichotomy of "efficiency v. privacy".

(5) End-to-End Security – Lifecycle Protection**:** In PbD, security is embedded into the system *ab initio*, and extends throughout the lifecycle of data processing. This extends the following FIP:

- *Security*: While security and privacy must not be conflated, security is indeed a pre-requisite for privacy. Data controllers must be accountable for adopting recognized security standards in the processing of data.

(6) Visibility and Transparency: Notwithstanding their rigour, the components and operation of systems and practices must be open to independent verification. This enforces the following FIPs:

- *Accountability*: Data controllers owe a duty of care to data subjects while processing their data.
- *Openness*: Information about data policies and practices must be freely accessible to users.

- *Compliance*: There must not only be a means for verifying compliance but also a redressal and appellate mechanism.

(7) Respect for User Privacy**:** The system must be consciously engineered in manner that makes it user centric and empowers them in the management of their own data. User privacy operationalizes:

- *Consent*: The consent must be free, fair, lawful, and revocable.
- *Accuracy*: Data collected must be complete and up-to date.
- *Access*: Users must have access to their data.
- *Compliance*: Means of verification and grievance redressal.

Evidently, PbD is holistic, interdisciplinary, integrative, and innovative, whilst also aptly shifts the primary accountability from the user to the data controller. Thus, this approach is extremely well-equipped in responding to the paradigm shift of the Fourth Industrial Revolution ("4th IR").

3.3 Addressing Criticism to PbD

3.3.1 Justifying intervention through Technological Design

A common criticism of PbD is that technology doesn't require intervention because it is value neutral. This conception is flawed because values are deeply embedded into technological design.[22] Design decisions establish power and authority. After we shape our tools, thereafter they shape us.[23] Given this inherently ethical nature of design, ignoring its regulation is sanctioning pervasive corporate control over people's lives. This is particularly problematic because bad design obscures harms and undermines user expectations of

[22] Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control Design of New Technologies* (HUP 2018) 14-15.

[23] Íbid 8.

privacy, leading to a paradox where users, despite awareness of poor privacy, continue using the service anyway.

Another line of critique is that intervention impedes the designer's prerogative to freely design. However, this freedom has never been absolute, neither can it ever be. The freedom to design while important, is not an objective good, and must be compromised in favor of protecting greater values like safety. Policymakers already intervene in design decisions, albeit in other fields, to protect such greater values. For instance, the mandatory safety requirements in automobiles, such as seatbelts and airbags, and architectural prescriptions for constructing buildings, like fire exits or ceiling heights. Given the extent of invasion and the role of design in facilitating this, privacy, a greater value, must similarly be prioritized through design intervention.

3.3.2 Criticism of vagueness and non-implementation

Cavoukian's model of PbD has been criticized as vague, leaving unanswered several questions as to their application to systems engineering.[24] Even its implementation is difficult,[25] because it merely outlines broad aspirational principles, without any specific guide to action. Despite the utility of Cavoukian's model in identifying an alternative path to data protection, and charting a broad roadmap therein, this criticism is valid.

However, this isn't an inherent limitation to PbD *per se*. These problems can be alleviated by adopting a comprehensive and specific methodology that bridges the gap between these principles and their contextual application.

---

[24] Jeroen van Rest, Daniel Boonstra, Maarten Everts, Martin van Rijn and Ron van Paassen 'Designing Privacy-by-Design' in Bart Preneel and Demosthenes Ikonomou (eds), *Privacy Technologies and Policy* (Springer 2012).

[25] Ira Rubinstein and Nathan Good, 'Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents' (2013) 28 BTLJ 1333, 1412-1413.

4 Operationalizing Privacy by Design through Privacy Engineering

The vagueness and implementational critiques to PbD can be addressed by adopting the methodology of privacy engineering ("PE"). It is a systematic and multi-layered approach that operationalizes the principles of PbD throughout the lifecycle of a system in specific use cases.

PE has three distinct stages, each with their own unique operational elements:

4.1 Privacy Requirements Definition

4.1.1 Goals

The privacy requirements desired from the system must be specified in terms of implementable properties and functionalities.[26] These requirements are derived from a broader understanding of privacy goals and their FIPs. Thus, privacy goals serve as entry points to the PE methodology by determining specific privacy requirements, which, in-turn, influence the next stages of design and verification.

Traditionally, risk assessment only looked at unauthorized access to and modification of personal data.[27] Therefore, privacy protection goals were limited to confidentiality (avoiding unauthorized access), integrity (preventing unauthorized modification), and availability (guaranteed access to data and systems).

---

[26] Massachusetts Institute of Technology Research and Engineering– Privacy Community of Practice, 'Privacy Engineering Framework' (July 2014) <https://www.mitre.org/sites/default/files/publications/14-2545-presentation-privacy-engineering-frameworkjuly2014.pdf> accessed 20 September 2020.

[27] Agencia Espanola Proteccion Datos, 'A Guide to Privacy by Design' (2019), 15 <https://www.aepd.es/es/documento/guia-privacidad-desde-diseno_en.pdf> accessed 22 January 2023.

However, as outlined earlier, the 4th IR has shifted paradigms such that there are unprecedented and greater risks to privacy. Therefore, there is a need to extend these goals to include:[28]

(1) Unlinkability: inhibiting interaction between distinct datasets to prevent unauthorized usage and profiling;
(2) Transparency: data processing must be clarified such that it can be understood by all parties involved during any stage of processing; and
(3) Intervenability: enabling users to intervene during any stage of processing and enforce any corrective action.

Each of these goals, in-turn, embody respective FIP.[29] Therefore, a goal-based analysis automatically secures compliance to FIPs.

4.1.2 Strategy and Tactics

Operationalizing privacy goals into specific privacy requirements happens through privacy design strategies. These are general approaches that specify distinct design or architectural goals.[30] While design strategies do not necessarily prescribe a specific structure for the system, they indeed limit its possible realizations.[31] Moreover, design strategies identify tactics for more detailed achievement of goals.[32] However, tactics are to be followed throughout the

---

28 Marit Hansen 'Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals' in Jan Camenisch, Bruno Crispo, Simone Fischer-Hübner, Ronald Leenes, and Giovanni Russello (eds), *Privacy and Identity Management for Life* (Springer 2011).

29 Agencia (n 27) 13-14.

30 Michael Colesky, Jaap-Henk Hoepman and Christiaan Hillen, 'A Critical Analysis of Privacy Design Strategies' (2016) IEEE Security and Privacy Workshops <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7527750> accessed 22 September 2020.

31 Ibid.

32 Ibid.

lifecycle of data processing.[33]

Presently, there are eight design strategies across two categories: data-oriented strategies and process-oriented strategies.[34] Below each strategy, its corresponding tactics have also been explained:[35]

4.1.2.1 Data-Oriented Strategies:[36]

This focuses on the technological aspects to PbD, and includes four strategies:

(1) **Minimize**: Processing the least amount of data by reducing the sample size or per capita volume of information.

- *Select*: processed data must only pertain to relevant subjects and attributes.
- *Exclude*: a blacklist of subjects and attributes irrelevant to processing.
- *Strip*: partially eliminate data when it becomes unnecessary.
- *Destroy*: completing deleting processed data when it becomes irrelevant, and ensuring non-recovery.

(2) **Hide**: Preventing exposure to processed data through necessary means.

- *Restrict*: preventing unauthorized contact to data.
- *Mix*: process data in large and random groups to prevent correlation.
- *Obfuscate*: make data unintelligible, in storage and transmission, to those unauthorized.
- *Dissociate*: eliminating correlation between independent datasets.

---

33 Agencia (n 27) 15.

34 Jaap-Henk Hoepman, *Privacy by Design: The Little Blue Book* (2020) 3-4.

35 Naturally, the extent of applicability of each of these strategies and their tactics will depend upon the context.

36 Agencia (n 27) 16-17.

(3) **Separate**: Process data in a manner that avoids correlation between independent datasets.

- *Isolate*: process data independently through different databases or physical systems.
- *Distribute*: partition data into different sub-sets while processing.

(4) **Abstract**: Limiting the degree of detail of processed data.

- *Summarize*: generalizing the data as intervals/ranges.
- *Group*: aggregate individual data into common groups.
- *Perturb*: approximating data or modifying it through "noise".

4.1.2.2 Process-Oriented Strategies:[37]

This focuses on the organizational aspects of PbD, and includes four strategies:

(1) **Inform**: Providing abundant clarity on purposes of processing data, also changes therein, and security breaches in a timely manner.

- *Supply*: provide extensive resources on processing of data and grievance redressal.
- *Explain*: clarifying supplied information in a succinct and comprehensible manner.
- *Notify*: alert user on any changes in already supplied information.

(2) **Control**: Provide users control over their data by operationalizing existing rights.

- *Consent*: collect consent in a lawful, informed, and fair manner.
- *Alert*: provide real-time notification for data processing.

---

[37] Ibid.

- *Choose*: allowing partial selection/exclusion of data from processing.
- *Update*: enabling easy rectification/modification of data to maintain accuracy.
- *Retract*: allowing subjects to quickly delete any/all of their processed data.

(3) **Enforce**: Ensuring data processing is compatible with stated purposes and extraneous legal obligations.

- *Create*: creating privacy policies.
- *Maintain*: creating necessary procedures and structures to implement privacy policies.
- *Uphold*: ensuring compliance, efficiency, and effectiveness of said policy.

(4) **Demonstrate**: Proving compliance to privacy policies and laws.

- *Log*: record every decision and all aspects related to it.
- *Audit*: conduct independent assessment of extent of compliance.
- *Report*: analyzing logged and audited information to periodically review improvements to protection measures.

Naturally, the extent of applicability of each of these strategies and their tactics will depend upon the context.

4.2 Privacy Design and Implementation

This stage involves designing the system architecture, consisting of structures that include elements, their properties, and the relationships among them.[38] While designers largely have creative freedom in designing architecture, two

[38] Agencia (n 27) 14-15.

particular choices are significant:[39] network centricity[40] and personal identifiability.[41] Privacy friendliness is inversely proportional to both.

After making these choices, developers need to design and develop elements within the architecture. At this stage, privacy design strategies manifest as more specific design patterns. These are a template of reusable solutions to address common and repeated privacy problems that appear in a specific context during product/systems design and development.[42] They help designers to solve problems by breaking it down into smaller bits for easier comprehension. Simultaneously, the pattern describes consequences of planned subdivision, thus allowing the designer to determine its application achieves the desired goal.[43] Notably, one design pattern can be used to address multiple design strategies.[44]

Finally, after designing the system, privacy enhancing technologies ("PETs") are used to operationalize privacy design patterns with a concrete information and communication technology.[45] PETs can be used as privacy protection tools, such as encryption or anonymization, or privacy management tools to inform and advise users on the processing of their data. Notably, a single PET can be used to implement multiple design pattern solutions.

---

39 Sarah Spiekermann and Lorrie Faith Cranor, 'Engineering Privacy' (2009) 35(1) IEEE TSE 67, 74-77.

40 Network centricity indicates the control a service provider has over the user's operations, and the extent to which a user's system relies on a centralized networked infrastructure.

41 Personal identifiability indicates the extent to which data can be directly correlated to a user.

42 Jaap-Henk Hoepman, 'Privacy Design Strategies' (29th International Information Security Conference, Marrakech, 2014).

43 ENISA (n 10) 16-18.

44 For instance, as we will see in the case of AA, the consent artefact design pattern operationalizes the strategies of minimize, separate, control, and inform.

45 Hoepman (n 42).

4.3 Privacy Verification and Validation

At this final stage, the proper implementation of the defined privacy requirements is verified and validated. This can be done by the organization using technological monitoring tools along with physical correspondence and/or allowing third parties to intervene through independent audits or making code open source.

5 Utility of Privacy Engineering

5.1 Proposed Scheme in Regulation

The utility of PE lies in ensuring PbD in specific use cases through layers of flexible abstract thinking that can be operationalized through a web of distinct yet interconnected sub-elements. It consists of two broad elements: (1) the theoretical element (privacy goals, FIPs, and Cavoukian's PbD principles); and (2) the operational element. The theory provides the conceptual foundation and a general normative framework on the key considerations. The operational element of PE manifests as design strategy, design tactics, design patterns, and PETs.

Given the recurrent nature of privacy challenges, especially within a sector/industry, the operational elements can be expressed as a "web of templates". The web commences at more abstract levels and ends with specific technological or organizational suggestions. Accordingly, the web begins at design strategies, which merges into more specific design tactics, which are in-turn operationalized through even more specific design patterns, which may themselves be further operationalized through a concrete PET.[46]

[46] This flow is not water-tight, in that one design tactic can be addressed by multiple design patterns or a single design pattern may address multiple design tactics. Notwithstanding

When constructing this web, regulators and data controllers must ask two questions: *first*, the relevancy of a design strategy; and *second*, the extent of data protection required. To ensure certainty over the data controller's extent of accountability, both questions must be answered prior to the commencement of any data processing.

There must be a presumption that all strategies are relevant, unless proved otherwise. To disprove relevancy of a strategy, and its concomitants in web, it must be shown that the purpose and importance of the project are legitimate yet incompatible with the strategy. For instance, as I will demonstrate for the Account Aggregator Framework, when the purpose for data sharing needs extremely accurate analysis, the "abstract" strategy becomes irrelevant.

The extent of data protection must consider the state of the current technology, the cost of implementation, the organization's financial position, the purpose, frequency, and volume of data processed, and the expected harms consequent to a breach. Determining these will automatically answer both the specific sub-element and the extent to which the entire web is to be used. For instance, as I will demonstrate for the Aarogya Setu Application, the government has presently only specified up till the tactic, without detailing the specific design pattern and PET used. Given its deep pockets, the growth of precise re-identification techniques, the flexibility of the contact tracking purpose towards accuracy, and the sensitive nature of health data, a full and comprehensive extension of the 'abstract' strategy web is needed.

To simplify compliance, responses to the two-fold question under this "web of templates" approach can be standardized based on use cases across the industry/sector. For instance, all digital mobile payments application or even digital financial service providers can be subjected to the same requirements.

---

this merging, conceptualizing PE as a web provides a method of visualizing abstract obligations into specific smaller parts.

This standardized response is the minimum standard of data protection that the specific organization must follow.

While standardizing, through research, the regulator can develop a good overview of the state of current technology, relevant data processing activities, and consequent harms of breach within specific use cases in a particular sector/industry. However, the financial position of the data controller is not always known while making these determinations. Thus, an exemption/reward structure can be developed to ensure widespread compliance. Organizations failing to satisfy the minimum standard of data protection within their use cases must apply for exemptions before relevant regulators seeking temporary exemptions. On the other hand, organizations exceeding the minimum standard can be incentivized through government issued privacy guarantee certifications or even tax rebates.

5.2 PbD under Existing Law

The two-fold question is already indirectly asked by regulations, where PbD is mandatory, like India and the EU.

5.2.1 European Union

In the EU, PbD is condensed into a more specific legal obligation within the GDPR called "data protection by design" and "data protection by default".[47] Regulators have viewed PbD as being the more high-level, over-arching and aspirational concept, with Article 25 being a more focused application of that

[47] European Data Protection Board (EDPB), 'Guidelines 4/2019 on Article 25: Data Protection by Design and Default' (2019) <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf> accessed 20 January 2022.

broad concept.[48] The considerations under Article 25 herein too coincidences almost entirely with the second question, as flagged above.

Specifically, for data protection by design, the enquiry is over "the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing".[49] Evidently, the duty is qualified by a pre-defined list of contextual factors.[50] It is pertinent to evaluate their meaning and scope.

State of the art requires an evaluation of the current progress in technology that is available in the market.[51] Thus, it is a dynamic concept that requires controllers to continuously be updated. The cost of implementation covers not only economic costs but also resources in general, including time and personnel. The position is clear that inability to bear costs does not excuse compliance.[52] Nature refers to the inherent characteristics of processing, scope refers to the size and range of processing, context refers to the circumstances that may influence the data subjects' expectations, and purpose refers to the aims of processing.[53] The GDPR requires controllers to undertake risk assessment, in terms of probability and seriousness of harm, on the rights of data subjects associated with

---

48 European Data Protection Supervisor (EDPS), 'Preliminary Opinion on privacy by design' (2018) Opinion 5/2018, 1-5 <https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf> accessed 20 January 2022; Andrew Clearwater and Brian Philbrook, 'Privacy by Design and GDPR: Putting Policy into Practice' (*CPO Magazine*, 29 June 2018) <https://www.cpomagazine.com/data-privacy/privacy-by-design-and-gdpr-putting-policy-into-practice/> accessed 20 January 2022.

49 General Data Protection Regulation 2018, art 25(1).

50 Lee A Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 1 Oslo Law Review 105, 115-117.

51 EDPB (n 47), 7-8; Ira Rubinstein and Nathaniel Good, 'The trouble with Article 25 (and how to fix it): the future of data protection by design and default,' (2020) 10 International Data Privacy Law 37, 40-42.

52 EDPB (n 47) 8-9; Rubinstein and Good (n 51) 42.

53 EDPB (n 47) 9.

their processing.[54] These factors have to be evaluated both when systems or practices are being designed as well as when the data is being processed.[55]

Notably, controllers have considerable freedom in selecting their safeguards, so long as desired goals are achieved.[56] The application of these factors will significantly be determined through data protection impact assessments ("DPIA").[57] But DPIAs are only mandatory when there is a likelihood of high risk to persons, while the data protection by design obligation is not. Thus, the latter is wider in application. Moreover, the obligation is not just technological but also organizational, in that compliance has to be baked into both software and hardware as well business strategies and organizational practices.[58]

Data protection by default is an extension of Cavoukian's 2nd principle. Specifically, it requires an evaluation of "the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility". Its objective and relevant factors, under Article 25(2), are distinct from data protection by design, under Article 25(1).[59] While the former is concerned with a wide range of data protection safeguards, the latter is focused on keeping data "lean and locked up". Moreover, the former is process-oriented in its focus on designing technology and strategy, while the latter is goal-oriented in its commitment to ensure minimum guaranteed protections as regards principles

54 Ibid 9-10.

55 Rubinstein and Good (n 51) 41-42.

56 Bert Jaap Koops and Ronald Leenes, 'Privacy regulation cannot be hardcoded. A critical comment on the "privacy by design" provision in data-protection law' (2014) 28 International Review of Law, Computers and Technology 159.

57 Bygrave (n 50) 115; EDPS (n 48) 8.

58 Lina Jasmontaite et al, 'Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR' (2018) 4 European Data Protection Law Review 168.

59 Bygrave (n 50) 115-117.

like data minimization, storage limitation, and security. With these differences outlined, it is pertinent to evaluate the contextual factors in Article 25(2).

The amount of personal data requires evaluation of qualitative and quantitative factors, including the volume of personal data, as well as the types, categories and level of detail of personal data required for the processing purposes.[60] The extent of their processing requires processing to be strictly limited to the necessary purposes. But importantly, merely because personal data is needed to fulfil a purpose does not mean that all types of, and frequencies of, processing operations may be carried out on said data. Data controllers must not exceed the boundaries of compatible purpose, mindful of the expectations of the data subjects.[61] The period of their storage requires data deletion after purpose is completed, with any further retention requiring objective justification and demonstration.[62] Their accessibility requires the data controllers to ensure both a limitation on the personnel who can access the personal data as well as its availability to those who need it when necessary.[63]

Despite its revolutionary shift in re-focusing accountability on data controllers, Article 25 primarily suffers from the problem of lack of clarity over the parameters and methodologies for achieving its goals.[64] This is amplified by a lack of continuous authoritative guidance on said parameters and methodologies.

5.2.2 India

In India, the DPB mandates every data controller to prepare a PbD policy containing seven components, which largely coincidence with the second

60 EDPB (n 47) 11-12.
61 Ibid.
62 Ibid.
63 EDPB (n 47) 12-13.
64 Rubinstein and Good (n 51) 40-42; Bygrave (n 50) 117-119.

question.[65] There is presently no interpretative guidance on any of these components. Subsequently, this policy may also then be approved by the Data Protection Authority.[66]

5.3 Unique Benefits of the PE Methodology

While these legal provisions equip the regulator to ask correct questions, in the absence of a specific and comprehensive methodology, answers will be vague and negotiations with data controllers will be complicated. Against these pertinent questions, the PE methodology provides the data controller and regulator with "a language to communicate".[67] This addresses the aforementioned limitation in Article 25, GDPR. They can establish their privacy obligations concretely by addressing the relevancy question, and then determining the extent to which the web must be operationalized for each strategy. The result of negotiation using this language is specific technological and organizational solutions for pre-identified generalized privacy problems.

This specificity also generates greater certainty in the data protection process. A PbD model ensures that just by proper compliance, data controllers would be serving a significant portion of their entire privacy obligations. Since these obligations are now concretely defined, as against status quo where only goals (not processes to achieve these goals) are defined, there is greater certainty in compliance for data controllers. This language provides data controllers with a handbook of privacy protecting strategies, which they can also visualize. Each sub-element in the "web of template" is a pre-vetted, thus reliable solution. Therefore, mere compliance with privacy obligations defined in terms of the

65 Data Protection Bill 2021, s 22(1).
66 Data Protection Bill 2011, s 22(2).
67 Julia Black, 'Regulatory Conversations' (2002) 29 Journal of Law and Society 163.

language of the "web of templates", generates trust among data subjects through the creation of high privacy expectations.

While resource challenges are inevitable for smaller organizations, they can be addressed by appropriately defining the minimum standard for data protection through consultations and impact surveys, or granting temporary exemptions. Moreover, a specific language to communicate is also crucial for the regulator to undertake institutional capacity building. When privacy obligations are defined through concrete templates, the regulator automatically narrows down the focus area. Through this, the regulator can mitigate resource challenges by prioritizing on providing necessary information about and access to the relevant design pattern and PET.

Initially, at least, compliance to this PbD approach, before commencing any data processing, may generate some delays for the organization. Privacy compliance-based delays are inevitable. Presently, they happen through long drawn litigations. There is greater social value in shifting this delay pre-commencement given the long-term ramifications of design on privacy, in that adopting PbD will reduce privacy violations itself. Moreover, continued use of this methodology will inevitably result in more certainty, within industries, as to the relevancy of a strategy and the necessary templates to expand the web.

6 Evaluating the Account Aggregator Framework and the Aarogya Setu Application

The operational element of PE not only provides an implementational framework, but also an ideal to normatively assess PbD compliance by a technological solution. Beginning with the two-fold question,[68] each

[68] As argued earlier, relevance will be presumed, unless conflict between purpose and strategy found. Even when both questions are affirmatively answered, it may emerge that that these

technological solution will be evaluated against how it operationalizes the interconnected web of privacy design strategies, tactics, pattern, and PETs.

For this assessment, I have chosen two Indian technological solutions: (1) the Account Aggregator Framework ("AA") because of its revolutionary approach to data democratization and uniquely Indian origin;[69] and (2) the Aarogya Setu Application ("AS") because the COVID-19 pandemic makes it immediately relevant, and there has been significant controversy in India as to its privacy compliance.

Through this analysis, I will also demonstrate the practical application of the proposed PE methodology.

6.1 Account Aggregator Framework

6.1.1 Background

AA is a sub-set of the India Stack project, which seeks to build a set of interrelated digital public goods.[70] The project can be understood as a series of layers: identity, authentication, payments, signature, and consent.[71] The consent layer is

strategies, albeit necessary, must be enforced outside the present architecture due to technical limitations.

69 The objective of this framework is to "invert the data equation", i.e., allow data subjects to use their own data stored by other entities (like banks) for process validation and verification, thus enabling them to avail services. While different countries have adopted their own methods to data inversion, AA is the most structured and wholistic manner of achieving this objective so far.

70 India Stack, 'About Data Empowerment and Protection Architecture (DEPA)' <https://www.indiastack.org/depa/> accessed 22 September 2020; Indian Journal of Law and Technology, 'Webinar: The Account Aggregator Framework: A Multidisciplinary Dialogue' (2021) Panel Discussion Report, 22-23 <https://ebf0b2f5-faf2-4127-bbe7-46f0589b5bd1.filesusr.com/ugd/066049_1c2dec3dbe3546698b506d18aa853ff3.pdf> accessed 20 January 2022.

71 Derryl D'Silva, Zuzana Filková, Frank Packer, and Siddharth Tiwari, 'The design of digital financial infrastructure: lessons from India' (Bank for International Settlements, December 2019) 8-10 <https://www.bis.org/publ/bppdf/bispap106.pdf> accessed 16 October 2020; Raghav Aggarwal, Ajit Shukla, Nitin Saxena, and Avneesh Singh, 'Account aggregators - putting the customer in charge' (*PwC*) <https://www.pwc.in/consulting/financial-

operationalized through the Data Empowerment and Protection Architecture ("DEPA").[72] DEPA seeks to reverse the data equation and provide users with democratized access, portability, and control over their own personal data.[73] Essentially, DEPA is a series of protocols, across technological, organizational, and legal elements, that can be followed and extended upon in more specific use cases.[74]

One such specific use case of DEPA is AA, which currently applies in the financial services sector, with recognition by four regulators.[75] The process comprises four stakeholders: financial information providers ("FIPs") who possess user data, financial information users ("FIUs") who require user data, users, and data access fiduciaries. A typical transaction flows as follows:

- The user requests good/service from FIUs;
- FIUs then send request to FIPs for access to user data for auditing and verification;
- After FIPs receive this request, they transmit the data to the data access fiduciaries;

services/fintech/fintech-insights/account-aggregators-putting-the-customer-in-charge.html> accessed 16 October 2020.

72 NITI, 'Data Empowerment And Protection Architecture' (2020) <https://www.niti.gov.in/sites/default/files/2020-09/DEPA-Book.pdf> accessed 20 January 2022; Shubham Ruhela, 'Data empowerment and protection architecture explained' (*Indian Software Product Industry Roundtable – iSPIRT*, 23 June) <https://pn.ispirt.in/dataempowerment-and-protection-architecture-explained-video/> accessed 16 October 2020.

73 D'Silva (n 71) 7.

74 Max Totsky, 'How India's DEPA Framework Uses Software to Empower Privacy Compliance' (*Association for Data and Cyber Governance*, 13 August 2021) <https://adcg.org/how-indias-depa-framework-uses-software-to-empower-privacy-compliance/> accessed 20 January 2022.

75 Staff Writer, 'From bank account opening to buying mutual funds, how 'Sahamati' can help you' (*LiveMint*, 3 August 2019) <https://www.livemint.com/money/personal-finance/from-bank-account-opening-to-buying-mutual-funds-how-sahamati-can-help-you-1564496684595.html> accessed 22 September 2020.

- The data access fiduciary manages consent for the user through the consent artefact by allowing her to provide specific consent at a click;[76]
- Post user approval, the requested data securely and efficiently reaches FIPs.

Recently, the Account Aggregator ecosystem went live. Finvu, OneMoney, NESL, and CAMS are the four AAs that are currently operating, with PhonePe, Perfios, and Yodlee receiving in-principle approval from the RBI.[77] On the banking side, HDFC Bank, ICICI Bank, Axis Bank, and IndusInd Bank are already offering limited financial services to customers in this ecosystem.[78] The State Bank of India, Federal Bank, Kotak Mahindra Bank, and IDFC First Bank are expected to join shortly. Additionally, two non-bank lenders- Bajaj Finance Ltd and DMI Finance- have also joined the network.[79]

6.1.2 Evaluating PbD

6.1.2.1 Minimize

The design pattern of consent artefact operationalizes the tactics of "select", "exclude", "strip" and "destroy". Essentially, it is a machine-readable electronic document, written in XML, that consists of five sections: identifier,[80] data,

[76] These data access fiduciaries, known as AAs, are business organizations that have to register as non-banking financial companies with the RBI. Their interaction with the consumer is through an application, whose interface is very similar to UPI applications.

[77] George Mathew, 'Account Aggregators: New framework to access, share financial data' (*Indian Express*, 8 September 2021) <https://indianexpress.com/article/explained/account-aggregators-new-framework-to-access-share-financial-data-7490966/> accessed 20 January 2022.

[78] Vishwanath Nair, 'Eight Banks To Go Live On Account Aggregator Ecosystem' (*Bloomberg Quint*, 2 September 2021) <https://www.bloombergquint.com/business/eight-banks-go-live-on-account-aggregator-ecosystem> accessed 20 January 2022.

[79] Ibid.

[80] This section uniquely identifies each of the four participants.

logging,[81] purpose,[82] and signature.[83] The data section specifies the parameters and scope of data sharing that a user consents to in any data sharing transaction.[84] Thus, the user herself can select relevant attributes, and the artefact's design itself excludes irrelevant attributes from consideration. The artefact allows users to stipulate a duration for data storage, thus requiring FIUs to subsequently delete data. However, this is not an automatic requirement, and can be evaded by storing the data on a parallel database. Executing data transfers through a "pod", which imposes automatic technological limitations on data expiry, as a pattern may solve this solution.[85] While replication through backdoor channels like screen or video recording will inevitably exist, their performance is now significantly onerous.

6.1.2.2 Hide

AA's usage of end-to-end encryption as a design pattern,[86] with cryptography as the PET, operationalizes the tactics of "restrict" and "obfuscate". Access to the processed data is available to only the FIPs, users, and, on consent, FIUs. Therefore, any access to this data is restricted for external parties, including data access fiduciaries themselves. Cryptography ensures that the shared data is adequately obfuscated, thus unintelligible to these parties.

---

81 This section logs every transaction and data flow.

82 This section specifies the purpose of the data access.

83 This section contains the user's unique digital authentication.

84 Ministry for Electronics and Information Technology, *Electronic Consent Framework-Technology Specifications Version 1.1* (unspecified) 4-6.

85 Inspiration can be taken from Tim Berners Lee's project 'Solid', wherein all information is stored in a 'Solid pod' that acts like a digital safe. This kind of decentralized architecture allows the user greater control over the manner and time period of data usage by the FIUs. *See* Frederiek Fernhout, 'Tim Berners-Lee's Solid proposal: the future of data traffic?' (*Stibbe*, 12th October 2018) <https://www.stibbe.com/en/news/2018/october/tim-bernerslees-solid-proposal-the-future-of-data-traffic> accessed 16 October 2020.

86 D'Silva (n 71) 24.

However, since data sharing happens individually, there is still scope for correlations. Given the sensitivity of financial information, the financial harms of breach, and the increasing ease through which algorithms can make predictions, greater operationalization of this strategy is needed. This can be done by using mix networks as a design pattern, which operationalizes the "dissociate" tactic. They add an additional layer of obfuscation by utilizing a chain of proxy servers that receive messages randomly from multiple sources, and then rearrange and resend them randomly to the next destination.[87] More importantly, they unlink end-to-end communications making it difficult to establish correlations and track communications.[88]

Since the shared data needs to be extremely accurate and individualistic, adopting the "mix" tactic, using generalisation/suppression techniques, becomes irrelevant.

6.1.2.3 Separate

Typically, the consent artefact allows the user to determine the scope of shared data. Thus, any extraneous data from other databases cannot be prejudicially used against them. However, this situation is compromised when the FIP and FIU are the same entity in the transfer. In these situations, the entity can comply with AA protocols, and after receipt of data, simply correlate it with other databases to prejudice users' control. Conscious users can overcome this by strategically using unrelated FIPs and FIUs, but this choice is definitely a luxury. In those cases, legal compensation is the only remedy.[89] Anyhow, this is a problem of the FIP/FIU's architectural limitations rather than that of AA. Thus,

---

87 Agencia (n 27) 41.

88 Ibid.

89 This can be sought under s. 43, Information Technology Act 2000 or s. 57, s. 58, s. 60, s. 65, Data Protection Bill 2021, after it is passed.

this strategy is mostly irrelevant for AA.

6.1.2.4 Abstract

This strategy is irrelevant for AA because the shared data needs to be extremely accurate and individualistic. While patterns such as differential privacy or aggregation gateways can be used, this is unnecessary because inaccurate data may be prejudicial to the user's availment of the requested service. Anyhow, by controlling the data flow, the consent artefact mitigates a large extent of behavioural profiling.

6.1.2.5 Control

The consent artefact operationalizes the tactics of "consent", "choose" and "retract". Its data section allows the user to determine the duration, life, frequency, and revocability of the shared data.[90] Additionally, it enables users to determine whether the shared data can be subsequently shared, and if so, then determine similar limitations on this subsequent transfer.[91] The purpose section clarifies the need for data sharing.

Even the revocation by user can be easily undertaken by contacting FIPs through an accessible revocation URL. Moreover, the user can granularly choose the type and extent of data being shared, even from the same document like a bank statement. Operationalizing these choices does not require any knowledge of coding. AA applications have a simple user interface which have a standardized and expandable set of options that can be clicked on to

---

[90] Parijat Ghosh, 'Nandan Nilekani's Sahamati For Account Aggregators – Sounds Like A Great Idea On Paper, Is India Inc Ready?' (*Decimal Tech*, 8 August 2019) <https://decimaltech.com/nandan-nilekanis-sahamati-for-account-aggregators-sounds-like-a-great-idea-on-paper-is-india-inc-ready/> accessed 22 September 2020.

[91] Ibid.

operationalize these choices. Therefore, not only is the consent informed, but it is the user who informs it.

AA's process design mandates and automates a real-time data access notification from the FIP to the user and also on its receipt by the FIUs,[92] thereby satisfying the "alert" tactic. Since the framework is only concerned with data sharing, not collection, there is no means to rectify and modify recorded data. Thus, the "update" tactic is not operationalized. To remedy this, the app can include a communication channel between the user and the FPI, through the AA app, where requests as to necessary updates can be timely and efficiently made. This can be achieved using the design patterns of "active broadcast of presence",[93] wherein users can actively choose to convey and broadcast updated data, or "private link",[94] wherein users have an unguessable URL through which they can communicate with data controllers. This would eliminate the need to separately contact FIPs.

6.1.2.6 Inform

The artefact contains all information regarding the shared data as standardized options that are easily comprehensible. These can also be further expanded by data conscious users through simple interactions on the app. The AA app also contains contact details for queries and grievances. All these aspects collectively satisfy the "supply" tactic. The "i" privacy icon, corresponding to each standardized option on the interface version of the consent artefact, is a design

---

92 Malvika Raghavan and Anubhutie Singh, 'Building Safe Consumer Data Infrastructure in India: Account Aggregators in the Financial Sector (Part-2)' (*Dvara Research*, 7 January 2020) <https://www.dvara.com/blog/2020/01/07/building-safe-consumer-data-infrastructure-in-india-account-aggregators-in-the-financial-sector-part-2/> accessed 16 October 2020.

93 'Active Broadcast of Presence' (*Privacy Patterns*) <https://privacypatterns.org/patterns/Active-broadcast-of-presence> accessed 16 October 2020.

94 'Private Link' (*Privacy Patterns*) <https://privacypatterns.org/patterns/Private-link> accessed 16 October 2020.

pattern that provides succinct and simple explainers, thereby utilizing the "explain" tactic. As there are never any changes in the data shared from the FIU or FIP end, the "notify" tactic is irrelevant here.

6.1.2.7 Enforce

Currently, all launched AA applications have a privacy policy.[95] Anyhow, the control provided by the artefact and a lack of data storage by the AA greatly reduces the necessity of a privacy policy. Except for CAMS Finserv, all other AAs have also appointed specific grievance officers, and published their contact details.[96] Thus, the "create" and "maintain" tactic, albeit reduced in need, are fully operationalized.

The consent artefact is an open standard,[97] allowing replicability and any third-party to verify compliance. Naturally, if the source code is correct, then the process can be trusted. This operationalizes the "uphold" tactic.

6.1.2.8 Demonstrate

The logging section reliably and immaculately records both data and consent flows. Therefore, every time a transfer happens successfully/unsuccessfully,

---

95 NESL, 'Privacy Policy' <https://www.nadl.co.in/wp-content/uploads/2021/03/9d_NADL_Privacy_Policy_220819.pdf> accessed 20 January 2022; Finvu, 'Privacy Policy' <https://finvu.in/privacy> accessed 20 January 2022; OneMoney, 'Privacy Policy' <https://docs.onemoney.in/resources/privacy-policy/> accessed 20 January 2022; CAMS Finserv, 'Privacy Policy' <https://www.camsfinserv.com/PrivacyPolicy> accessed 20 January 2022.

96 NESL, 'Grievance Redressal' <https://www.nadl.co.in/grievance-redressal/> accessed 20 January 2022; Finvu, 'Grievance Redressal' <https://finvu.in/grievance> accessed 20 January 2022; OneMoney, 'Terms of Use: Contact Onemoney' <https://docs.onemoney.in/resources/onemoney-terms-of-use/> accessed 20 January 2022; CAMS, 'Grievances' <https://www.camsonline.com/Investors/Support/Grievances> accessed 20 January 2022: however, this is not specific to CAMS' AA, and there is also no specific individual assigned.

97 Ruhela (n 72).

audit logs are created.[98] This operationalizes the "log" tactic. The RBI mandates AAs to conduct any audits at least once in two years by CISA certified external auditors, with the reports being submitted to the Regional Office of the Department of Supervision of the concerned Bank.[99] AAs also have to establish an Audit Committee, consisting of not less than three members of its Board of Directors.[100]

These requirements are in line with the fact that the entire business model of data access fiduciaries is based on protecting the consumer; therefore, it is in their business interest to conduct independent audits and review potential improvements to the infrastructure and service delivery. Moreover, independent auditing can be conducted through the source code. In these ways, AAs operationalize the "audit" and "report" tactics.

In summation, AA exceptionally embodies PbD.

6.2 Aarogya Setu Application

6.2.1 Background

AS was developed by the National Informatics Center, under the Ministry of Electronics and Information Technology, to combat the COVID-19 pandemic in India.[101] Its purpose is to serve as a tool for: contact tracing,[102] syndromic

98 Ghosh (n 90).

99 Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions 2016, para 8(f).

100 Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions 2016, para 14.2.

101 The Hindu Net Desk, 'How does the Aarogya Setu app work?' (*The Hindu*, 8 May 2020) <https://www.thehindu.com/news/national/how-does-the-aarogya-setu-app-work/article31532073.ece> accessed 22 September 2020.

102 Terms of Service, Aarogya Setu Application, cl. 1.

mapping,[103] COVID-19 information,[104] self-assessment,[105] and e-passes.[106] AS is available in 12 languages over Android, iOS, and KaiOS platforms.[107] Aggressive governmental and private sector promotion has seen its downloads cross 150 million users.[108] However, its adoption has raised widespread and vociferous privacy concerns. Relevant privacy information has been expressed through a thrice-revised privacy policy,[109] and a Data Access and Knowledge Sharing Protocol ("the Protocol").

6.2.2 Evaluating PbD

6.2.2.1 Minimize

AS' design operationalizes the tactics of "select" and "exclude". It collects four pieces of data ("response data"): personal identifiers,[110] GPS location,[111] Bluetooth ID,[112] and self-assessment test details.[113] Each of these are relevant for a different AS purpose: personal identifiers and GPS location help in detailed and nuanced

---

103 Ibid.

104 Ibid.

105 Ibid.

106 Ibid.

107 Ministry of Electronics and Information Technology, 'Aarogya Setu is now open source' (*PIB*, 26 May 2020) <https://pib.gov.in/PressReleasePage.aspx?PRID=1626979> accessed 22 September 2020.

108 Harsh Upadhyay, 'Aarogya Setu app enters 150 Mn user club in 4 months' (*Entracker*, 12 August 2020) <https://entrackr.com/2020/08/aarogya-setu-app-enters-150-mn-user-club-in-4-months/> accessed 22 September 2020; Google Play, 'Aarogya Setu' <https://play.google.com/store/apps/details?id=nic.goi.aarogyasetu&hl=en_IN&gl=US> accessed 20 January 2022.

109 The paper will review the current, not original, form of the privacy policy and design features. In fact, this progressively changing nature of policy and design is an embodiment of PbD. It is difficult, especially for large scale projects like AS, to implement perfect designs and policies. Thus, self-improvement is intrinsic to effective PbD.

110 This is further split into demographics and contact details; Privacy Policy, Aarogya Setu Application, cl. 1(a).

111 Privacy Policy, Aarogya Setu Application, cl. 1(a), 1(b), and 1(c).

112 Ibid.

113 Privacy Policy, Aarogya Setu Application, cl. 1(c) and 1(d).

syndromic mapping; test details enable non-medical self-diagnosis; Bluetooth ID, test results, and mobile number help in contact identification and follow-up; and personal identifiers and ID proof information for vaccine registration- though this is optional. In this way, AS' design selects data based on a "white list" of requirements, with all other data automatically in a "black list", thus eliminates the scope for processing any other data.

Locational, test, and contact data is purged from the app after 30 days of collection.[114] On the servers, it is purged within 45 days of collection if user is COVID-negative,[115] or within 60 days after cure if user is COVID-positive.[116] This is in-turn subject to a broader limit of 180 days from collection.[117] However, this may be extended if the Empowered Group approves.[118] Demographic data is stored so long as the account exists and if medical/administrative interventions have commenced.[119] This is in-turn subject to a broader limit of the life of the Protocol. However, if users make prior request, then this,[120] and all other data must be deleted within 30 days.[121] However, these retention deadlines do not apply to anonymized and aggregated datasets.

Thus, by sequentially and automatically deleting unnecessary response data after reasonably set time periods, the "destroy" and "strip" tactics are operationalized. However, as I argue under "abstract", such deletion is not irreversible.

---

114 Privacy Policy, Aarogya Setu Application, cl. 3(b).
115 Ibid.
116 Ibid.
117 Privacy Policy, Aarogya Setu Application, cl. 5(e); Aarogya Setu Data Access and Knowledge Sharing Protocol 2020, cl. 7(a).
118 Ibid.
119 Privacy Policy, Aarogya Setu Application, cl. 3(a).
120 Aarogya Setu Data Access and Knowledge Sharing Protocol 2020, cl. 5(e).
121 Privacy Policy, Aarogya Setu Application, cl. 4(b).

6.2.2.2 Hide

Response data is shared with relevant/necessary persons to carryout required medical/administrative interventions.[122] Such persons must belong to concerned health ministries/departments at any level or authorities needing such data strictly for appropriate health responses.[123] In de-identified form, it can be shared with ministries/departments at any level or disaster management authorities or public health institutions so long as it for formulation/implementation of critical health response.[124] NIC is required to document the agencies/persons, time, and categories of data shared.[125] However, this is only "to the extent reasonable".[126] Given the sensitivity of the collected data and scope for misuse, the extent of data protection needs to be broadened. This can be done by converting documentation into a binding legal obligation. In rare cases, the need for secrecy and accountability can balanced through in-camera proceedings.

Even third-party transfers are allowed only for appropriate health responses, but with the same obligations as the sharing authority, who are still liable for them.[127] Designated category of research institutes,[128] are provided access only to "hard anonymized" forms of such data.[129] Moreover, they are still subject to government audits.[130] Thus, except for the standard of documentation, AS operationalizes the "restrict" tactic.

---

122 Privacy Policy, Aarogya Setu Application, cl. 2(a).
123 Aarogya Setu Data Access and Knowledge Sharing Protocol 2020, cl. 6(a).
124 Aarogya Setu Data Access and Knowledge Sharing Protocol 2020, cl. 6(b).
125 Aarogya Setu Data Access and Knowledge Sharing Protocol 2020, cl. 6(c).
126 Aarogya Setu Data Access and Knowledge Sharing Protocol 2020, cl. 6(c).
127 Aarogya Setu Data Access and Knowledge Sharing Protocol 2020, cl. 7(b).
128 Aarogya Setu Data Access and Knowledge Sharing Protocol 2020, cl. 8(c), 8(d), and 8(e).
129 Aarogya Setu Data Access and Knowledge Sharing Protocol 2020, cl. 8(a) and 8(b).
130 Aarogya Setu Data Access and Knowledge Sharing Protocol 2020, cl. 8(f).

The processed data is encrypted both in transit and at rest using "Advanced Encryption Standard".[131] Even deciphering this doesn't allow attackers access to user's data, as local data storage on device is anonymized too.[132] However, the demographic data uploaded onto servers through a unique ID is without any obfuscation.[133] This is a downgrade from earlier requirement of hashing such ID in static form.[134] The sensitivity of collected information and increasing interception attacks necessitate greater protection. To this end, AS must utilize dynamic IDs, which randomly change every 15 minutes, to prevent sniffing/replay attacks.[135] The need for this is mitigated, albeit not eliminated, due to the sheer volume of processed data.[136] In this way, AS, partly, operationalizes the "obfuscate" tactic.

Alike AA, AS can use mix networks to operationalize the "dissociate" tactic to minimize correlation.

6.2.2.3 Separate

The demographic and test data, and locational data at those points, are automatically stored on the central server.[137] The Bluetooth IDs exchange,[138] and

131 Ministry of Electronics and Information Technology, 'Aarogya Setu Technical FAQs' (26 May 2020) <https://static.mygov.in/rest/s3fs-public/mygov_159056968451307401.pdf> accessed 22 September 2020.

132 Ibid.

133 SFLC, 'Our Analysis of Aarogya Setu's Updated Privacy Policy and Terms of Service' (26 May 2020) <https://sflc.in/our-analysis-aarogya-setus-updated-privacy-policy-and-terms-service> accessed 22 September 2020.

134 Ibid.

135 Anand Venkatanarayanan, 'Covid-19: How The Aarogya Setu App Handles Your Data' (*Bloomberg Quint*, 17 April 2020) <https://www.bloombergquint.com/coronavirus-outbreak/covid-19-how-the-aarogya-setu-app-handles-your-data> accessed 22 September 2020.

136 However, malignant actors can still target pre-identified specific persons. Dynamic IDs prevent such cases.

137 Privacy Policy, Aarogya Setu Application, cl. 1(a) and 1(c).

138 Privacy Policy, Aarogya Setu Application, cl. 1(b).

locational data is stored on users' devices.[139] Former is uploaded to server only when contacted user turns positive,[140] while latter when user herself tests positive or has high risk of infection corresponding to self-assessment test.[141] Presently, only 0.1% of all users' contact tracing data has been uploaded to the server.[142] Thus, AS' architectural design operationalizes the "distribute" and "isolate" tactics by processing data over physically independent systems in different sub-sets.

However, once all data is uploaded centrally, correlation is possible using government or private-sector databases. Though, this is an architectural problem outside AS. Concerningly, as a last resort, availability of legal compensation is unclear.[143]

6.2.2.4 Abstract

Given the importance of accuracy, this strategy is irrelevant for AS' purpose of contact-tracing and self-assessment. However, it finds use for syndromic mapping, where some accuracy can be compromised. For this, users' demographic[144] and locational data[145] is used to prepare anonymized and aggregated datasets. Thus, the tactic of "group" is operationalized. However, the

---

139 Privacy Policy, Aarogya Setu Application, cl. 1(d); Aarogya Setu Data Access and Knowledge Sharing Protocol 2020, cl. 5(d).

140 Privacy Policy, Aarogya Setu Application, cl. 2(b).

141 Privacy Policy, Aarogya Setu Application, cl. 2(d)

142 Vidhi Desk, 'Aarogya Setu's Data Access and Knowledge Sharing Protocol, 2020: An explainer by the Vidhi Centre for Legal Policy' (*Vidhi Center for Legal Policy*, 11 May 2020) <https://vidhilegalpolicy.in/blog/aarogya-setus-data-access-and-knowledge-sharing-protocol-2020/> accessed 22 September 2020.

143 Given that S. 43A ITA only provides compensation against "body corporates"- which won't include these respective State departments/ministries- legal compensation may be unattainable under this provision. However, paragraph 6 of Terms of Services (3.0) only limits government liability over accuracy of identification and notification. Thus, unauthorized usage may be remediable as a contractual violation in court.

144 Privacy Policy, Aarogya Setu Application, cl. 2(a).

145 Privacy Policy, Aarogya Setu Application, cl. 2(c).

specific design pattern, and PET, used is unspecified.

This is particularly important because of the sensitivity of the collected data, and re-identification through such datasets is possible if ordinary design patterns used.[146] Herein, the tactics of "perturb" and "summarize" need to be operationalized. The design pattern of differential privacy can be used to add "noise" to final data, especially profession and age intervals.[147] Furthermore, the design pattern of "dynamic location granularity" can be used to reduce locational granularity from street to area/city.[148] However, these have to be balanced against need for precision in sex, age, and travel data.

6.2.2.5 Inform

The "supply" tactic is operationalized through a comprehensive and simple privacy policy, terms of service, and the Protocol. The presentation of information in this manner operationalizes the design pattern of abridged terms and conditions.

The policy and service terms are easily found on the app. Moreover, all privacy relevant questions have been separately answered in an "FAQ" sub-section, in each of the 12 languages, which is viewable on limited scrolling through the home section. Even the collection of information at registration is accompanied by an "i" privacy icon for user's ease of reference. However, the

---

146 Gayathri Vaidyanathan, 'Aarogya Setu: Major Surveillance, Few Safeguards In Modi Govt COVID Tracking App' (*HuffPost*, 10 April 2020) <https://www.huffingtonpost.in/entry/aarogya-setu-surveillance-covid-tracking-app_in_5e8d6e26c5b6e1d10a6bdea6> accessed 22 September 2020; Alex Hern, ''Anonymised' data can never be totally anonymous, says study' (*The Guardian*, 23 July 2019) <https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds> accessed 22 September 2020.

147 Adding 'noise' entails randomly changing correct pieces of information into incorrect data, and also determining the extent of deviancy of such incorrectness.

148 Privacy Patterns, 'Location Granularity' <https://privacypatterns.org/patterns/Location-granularity> accessed 22 September 2020.

usage of both a privacy policy and protocol on the same issues complicates understanding for a lay-user. Additionally, the relationship between the two is unclarified, and there are inconsistencies between them.[149] Thus, barring multiplicity of and some inconsistencies between documents, the "explain" tactic is operationalized.

The first two changes in privacy policy and service terms were not notified only,[150] while the third change saw delayed notification.[151] However, subsequently, the design pattern of asynchronous notice has been used, wherein consent to revised term and policy changes is automatically necessary for continued availment. Thus, there only needs to be greater promptness to fully operationalize the "notify" tactic.

6.2.2.6 Control

User consent is collected in a lawful, informed, and fair manner. This consent can be extended to permit third-parties access to health status through the "Open API Services Portal".[152] The "retract" tactic is operationalized by allowing users to delete all their data, immediately from the app and within 30 days from the

---

[149] For instance, the privacy policy requires that personal data of user who has tested positive be purged after 60 days of her treatment and within 30 days of collection for user who has not been tested positive. On the other hand, the protocol provides a larger limit of 180 days since collection, regardless of former or latter. While this may be justifiable for former (180 days could serve as a broader upper-limit, thus even if treatment extends beyond this period, the 60-day limit of the policy could be infructuous, making retention for another 60 days after treatment impermissible), it is plainly inconsistent with the latter.

[150] HT Correspondent, 'Aarogya Setu privacy policy updated: What's new' (*Hindustan Times Tech*, 17 April 2020) <https://www.hindustantimes.com/tech/aarogya-setu-app-updates-privacy-policy-what-s-new/story-mEklzeoSq1XVZ16CYkYPRM.html> accessed 22 September 2020.

[151] Siddharth Sonkar, 'Guest Report: Bridging Concerns with Recommending Aarogya Setu' (*The Centre for Internet and Society*, 20 June 2020) <https://cis-india.org/aarogya%20setu%20privacy> accessed 22 September 2020.

[152] Aditi Agarwal, 'Aarogya Setu launches Open API Services Portal: All you need to know' (*Medianama*, 22 August 2020) <https://www.medianama.com/2020/08/223-aarogya-setu-open-api-services/> accessed 22 September 2020.

servers, by simply deregistering through the settings section.

Since all collected data is important, the "choose" tactic is irrelevant for AS. However, AS needs to operationalize the "alert" tactic by providing notification to users every time their data is uploaded to or purged from the servers. Moreover, the design pattern of "data breach notifications" must be used to keep user informed and in control.[153] Optionally, alerts could be provided as to the authorities/persons viewing such data. Since response data is unaltered,[154] the "update" tactic is irrelevant. However, there must be scope for updating mobile number.[155]

6.2.2.7 Enforce

Necessary privacy documents satisfy the "create" tactic. However, the "maintain" and "uphold" tactics are only partly operationalized.

A grievance officer and his contact details have been shared,[156] but the precise procedure and timeline thereof is unclarified. The government has announced a bug bounty program for AS' Android version of up to ₹ 3 lakh for three categories of security vulnerabilities, and up to ₹ 1 lakh for suggestions towards source code improvements.[157] However, this program must be extended to iOS and KaiOS versions, and foreign researchers too for greater premium.

---

153 'Data Breach Notification Pattern' (*Privacy Patterns*) <https://privacypatterns.org/patterns/Data-breach-notification-pattern> accessed 22 September 2020.

154 Locational changes are self-administered by the app, self-assessment results are updated every time user volunteers to take a new test, and demographic details remain constant.

155 Currently, if a user changes his/her number, he/she will have to open a new account with that new number. This increase amount and surface area of data processed.

156 Privacy Policy, Aarogya Setu Application, cl. 7.

157 Ministry of Electronics and Information Technology, 'Aarogya Setu Bug Bounty Program: for Android Phones' (27 May 2020) <https://aarogyasetu.gov.in/wp-content/uploads/2020/06/mygov-999999999712190290.pdf> accessed 22 September 2020.

After repeated requests, the government made AS' Android version,[158] and later iOS version, open source.[159] However, presently, this is inadequate for meaningful verification due to three reasons. *Firstly*, the code repository remains stagnated since its release, with a huge backlog of queries and flagged issues.[160] *Secondly*, the server-side code has not been released. Given that most of AS' important functions are stored and performed on the server, not the device, little can be gathered without the server-side code.[161] *Thirdly*, the KaiOS version is not open source yet. Since this OS is available on the cheapest devices and has over 55 million users,[162] making it open source will significantly broaden transparency. Some of these limitations can be mitigated by reverse engineering the source code, however, this is complex and not fully accurate.[163] Anyhow, a project of this magnitude must ensure easy access to transparency. This can be done by: making KaiOS open source, sharing the server-side code, frequently updating source code, and regular engagement with developer queries.

Moreover, the government's failure to provide information about the process of creation of the App only adds to the existing scepticism over

158 Ministry of Electronics and Information Technology (n 107).

159 Prasid Banerjee, 'India open sources code for Aarogya Setu iOS app' (*LiveMint*, 13 August 2020) <https://www.livemint.com/technology/tech-news/india-open-sources-code-for-aarogya-setu-ios-app-11597321681940.html> accessed 22 September 2020.

160 Internet Freedom Foundation, 'Four months on, Aarogya Setu is still not open-source. WHY and WHEN is what the nation really wants to know!' (19 August 2020) <https://internetfreedom.in/aarogya-setu-should-be-open-source-now/> accessed 22 September 2020.

161 Ibid.

162 Aditi Agarwal, 'Aarogya Setu open sources its Android code, code now available on GitHub: Major win for privacy, accountability' (*Medianama*, 26 May 2020) <https://www.medianama.com/2020/05/223-aarogya-setu-code-open-sourced/> accessed 22 September 2020.

163 Regina Mihindukulasuriya, 'Source code and privacy — how Aarogya Setu compares with contract-tracing apps of 5 nations' (*The Print*, 26 May 2020) <https://theprint.in/tech/source-code-privacy-how-aarogya-setu-compares-with-contract-tracing-apps-of-5-nations/426375/> accessed 22 September 2020.

inadequate safeguards.[164] This has been compounded by their evasion of RTI questions regarding the App,[165] and their refusal to the let the concerned RTI activist attend the show cause hearing.[166] The Delhi High Court had to intervene to issue a notice to the Public Information Officers of several ministries, who later apologized.[167] Thus, the user has to blindly rely on the good conscience of government officials to adhere to its own policy.[168]

Finally, even meaningful open sourcing will not result in algorithmic transparency.[169] Thus, the AS team must publicize the prediction model of its algorithms.

6.2.2.8 Demonstrate

Organizational decisions are not always logged. Thus, the "log" tactic can be operationalized by obligating recording of all organizational decisions, at least for *post facto* in-camera proceedings.

AS' team conducts a thorough security audit through academicians, audit companies, and ethical hackers before each updated version is released.[170]

---

164 Gaurav Vivek Bhatnagar, 'Centre Apologises for 'Irresponsible Submissions' Regarding Aarogya Setu Before CIC' (*The Wire*, 8 December 2020) <https://thewire.in/government/centre-irrespinsible-submissions-aarogya-setu-rti-response> accessed 20 January 2022.

165 Internet Freedom Foundation, 'A look at Aarogya Setu through the Right to Information lens' (27 May 2020) <https://internetfreedom.in/aarogya-setu-through-the-right-to-information-lens/> accessed 20 January 2022.

166 Internet Freedom Foundation, 'Govt officials to justify denial of information about Aarogya Setu in secret hearing before CIC' (23 November 2020) <https://internetfreedom.in/cic-legal-notice-aarogya-setu-show-cause-hearing/> accessed 20 January 2022.

167 Internet Freedom Foundation, 'Delhi HC issues notice to govt in petition challenging denial of RTI regarding Aarogya Setu' (19 January 2021) <https://internetfreedom.in/delhi-hc-hearing-aarogya-setu/> accessed 20 January 2022.

168 Ankit Kapoor, 'Aarogya Setu Application: Design, Practice, and Infringed Constitutional Values' (*Centre For Information Communication and Technology Law*, 18 August 2021) <http://ijcl.co.in/index.php/2021/08/18/aarogya-setu-application-design-practice-and-infringed-constitutional-values/#_edn42> accessed 20 January 2022.

169 Sonkar (n 151) 17-21.

170 Ministry of Electronics and Information Technology (n 131).

However, the "audit" tactic can be fully operationalized if these audits are extended to organizational practices too, and with greater public transparency about the findings in both such audits. This tactic is particularly relevant given incidents of public declaration of name and contact details of COVID-19 patients from the AS app in Ahmedabad, Karnataka, and Punjab.[171] Moreover, the Jammu and Kashmir administration has shared the app's data with law enforcement agencies.[172]

AS' team has been fairly responsive to internal audits and legitimate public criticism of design and policy. This has resulted in three updates to the privacy policy and service terms, the protocol's release, and small wins in open-sourcing. However, the frequency of responses, and design changes mentioned herein, can be significantly improved to fully operationalize the "report" tactic.

In summation, AS averagely embodies PbD.

7 Legal Framework underpinning these Applications

Notwithstanding the transformative utility of organizational and technological design in addressing privacy and data protection issues, legal frameworks are still relevant and important. This is because they not only provide clarity and certainty over rights and obligations but also a means and procedure for redressal in the event of non-compliance. They also signal to stakeholders to discharge their obligations with sincerity, with the ensuing penalties serving as adequate deterrents. Since no design solution is immaculate, the law will always

---

171 Internet Freedom Foundation, 'Privacy prescriptions for technology interventions on Covid-19 in India' (2020) IFF Working Paper No 3, para 2.4-2.6.

172 Bisma Bhat, 'Breach of Privacy? JK Admin shared user data collected through Aarogya Setu App with Police' (*FreePressKashmir*, 20 March 2021) <https://freepresskashmir.news/2021/03/30/breach-of-privacy-jk-admin-shared-user-data-collected-though-aarogya-setu-app-with-police/> accessed 20 January 2022.

be a useful last-stage tool.

Against this context, it is useful to examine the legal frameworks underpinning both AS and AA.

7.1 Account Aggregators

The rights, obligations, and procedure detailed in the preceding section have been recognized and established in the RBI Master Directive Non-Banking Financial Company- Account Aggregator (Reserve Bank) Directions, 2016.[173] This directive has been last updated on 5th October, 2021, and was issued by the RBI in exercise of their powers under S. 45JA, the Reserve Bank of India Act 1934.[174] While the Directive remains silent on the consequence of non-compliance, the RBI under its parent Act is generally empowered to penalize AAs, in their capacity as Non-Banking Financial Companies, through imprisonment or fines.[175] However, there appears to be no legal basis to issue specific directions or revoke the issued licenses.

7.2 Aarogya Setu

The legality of AS has been a question of immense public debate. In *KS Puttaswamy v. Union of India*,[176] the Supreme Court of India recognized the right to privacy as a fundamental right, enforceable against the state. It established a four-fold test for its infringement: legality, legitimate goal, proportionality, and

---

[173] RBI, 'Master Directive Non-Banking Financial Company- Account Aggregator (Reserve Bank) Directions, 2016' <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10598> accessed 22 January 2023; Malavika Raghavan and Anubhutie Singh, 'Regulation of information flows as Central Bank functions? Implications from the treatment of Account Aggregators by the Reserve Bank of India' (2020) Central Bank of the Future Conference, Gerald R Ford School of Public Policy, University of Michigan.

[174] Ibid.

[175] Reserve Bank of India Act 1934, s. 58B.

[176] (2017) 10 SCC 1.

procedural safeguards.[177]

On legality, it noted that the infringement of personal privacy by the state must be through a valid and existent law. However, the government has not passed any legislation or promulgated any ordinance specifically for the App. Therefore, the question is whether it has the power to do so under any existing legislations. So far, the government has invoked the Epidemic Diseases Act, 1897, and the Disaster Management Act, 2005 to justify its actions in containing COVID-19.[178]

The 1897 Act empowers the central government to frame regulations during epidemics if the existing law is insufficient. However, this conferral is authorized in the limited context of inspecting vessels at ports, and detaining people for the same. Thus, there is no power to curtail the right to privacy under this Act.

The 2005 Act empowers the central government to take all such measures as it deems necessary or expedient for the purpose of disaster management. The term disaster, under Section 2(d), does not ordinarily extend to epidemics. However, on 14 March, the Home Affairs Ministry declared the coronavirus outbreak as a "notified disaster", thus bringing it within the fold of Section 2(d).[179] Therefore, releasing an app to contain COVID-19 would be within the powers of the government within the Act.

However, the sweeping powers under this Act make direct and collateral privacy breaches more susceptible. Considering this, the government must

---

177 While the first three prongs are mandatory, the fourth is only recommendatory or normative.

178 Gautam Bhatia, 'An Executive Emergency: India's Response to Covid-19' (*Verfassungsblog*, 13 April 2020) <https://verfassungsblog.de/an-executive-emergency-indias-response-to-covid-19/> accessed 20 January 2022.

179 FP Staff, 'Coronavirus Outbreak: The Disaster Management Act explained' (*Firstpost*, 26 March 2020) <https://www.firstpost.com/health/coronavirus-outbreak-disaster-management-act-provides-legal-backing-for-punitive-measures-allows-govt-to-access-emergency-funds-all-you-need-to-know-8190161.html> accessed 20 January 2022.

consider framing a specific law. Even BN Srikrishna, a former Supreme Court judge and the Chairperson of the Commission on India's data protection bill, had recommended the existence of a specific law.[180] This is especially since there is ambiguity over the enforceability of privacy policies,[181] and in any case, the ensuing practical difficulties associated with litigation deter initiation of any cause of action. Even the Protocol is problematic since it is in the nature of an executive order, thereby evading any necessary parliamentary scrutiny.

Originally, the government had declared the installation of the app to be mandatory.[182] However, on backlash, they have obligated employers to ensure compliance on a "best efforts" basis instead.[183] In practice, the government, and many private players due to the threat of non-compliance, have still insisted on mandatory usage of the app, without passing any specific legislation.[184]

---

180 Akshita Saxena, '"It Causes More Concern To Citizens Than Benefit': Justice BN Srikrishna Says 'Mandating The Use Of Arogya Setu App Is "Utterly Illegal"' (*LiveLaw*, 12 May 2020) <https://www.livelaw.in/top-stories/justice-bn-srikrishna-says-mandating-the-use-of-arogya-setu-app-is-utterly-illegalwatch-video-156629> accessed 20 January 2022.

181 Kapoor (n 165); Myanna Dellinger, 'Is a Website's Privacy Policy a Binding Contract?' (*ContractsProf Blog*, 10 August 2010) <https://lawprofessors.typepad.com/contractsprof_blog/2010/08/is-a-websites-privacy-policy-a-binding-contract.html> accessed 20 January 2022.

182 Danny Cyril D Cruze, 'Aarogya Setu now mandatory for employees in India' (*Livemint*, 2 May 2020) <https://www.livemint.com/news/india/aarogya-setu-now-mandatory-for-employees-in-india-here-s-how-to-register-11588408846545.html> accessed 20 January 2022.

183 Ministry of Home Affairs, Order No. 40-3/2020-DM-I(A), dated 27th January 2021 <https://www.mha.gov.in/sites/default/files/MHAorderdt_27012021.pdf>; Ministry of Home Affairs, Order No. 40-3/2020-DM-I(A), dated 30th September 2020 <https://www.mha.gov.in/sites/default/files/MHAOrderDt_30092020.pdf>; ET Bureau, 'Mandatory to best effort basis: Aarogya Setu app rule eased for companies (*The Economic Times*, 18 May 2020) <https://economictimes.indiatimes.com/tech/internet/mandatory-to-best-effort-basis-aarogya-setu-app-rule-eased-for-cos/articleshow/75794985.cms?from=mdr> accessed 20 January 2022.

184 Tanisha Ranjit, 'Aarogya Setu: Mandatory or not? We traced it for eleven months through our Tracker' (*Internet Democracy Project*, 22 April 2021) <https://internetdemocracy.in/2021/04/aarogya-setu-mandatory-or-not-we-traced-it-for-ten-months-through-our-tracker> accessed 20 January 2022.

8 Conclusion

Changes in the inherent value and usability of data in the 4th IR render the "consent framework" inadequate, thus necessitating the adoption of more holistic, innovative, and interdisciplinary regulatory approaches. Given its revolutionary approach to risk management and accountability shifts, PbD fits the bill. Since design decisions are inherently ethical, regulators are not only allowed but also morally obligated to intervene therein. However, the original model of PbD suffers from implementational challenges. This can be addressed by using Privacy Engineering as the revised methodology.

PE contains a theoretical element (privacy goals, Cavoukian's principles, and FIPs) and an operational element (design strategies, design tactics, design patterns, and PETs). The theoretical element is static and merely represents the consolidated understanding of existing privacy jurisprudence. The operational element operationalizes this theoretical understanding in specific use cases through layers of flexible abstract thinking, interconnected through a web of templates. Each sub-element is a template by itself, which can also be standardized for specific use cases within industries/sectors.

This "web of templates" can be constructed by answering the two-fold question of relevancy and extent of data protection required. Relevancy is understood as compatibility between purpose of project and concerned design strategy. The extent of data protection needs to be based on the state of technology, cost of implementation, financial position, the purpose, frequency, and volume of data processed, and the expected harms consequent to a breach. While existing legislations partly ask the second question, the absence of concrete methodology renders responses vague. In light of this, PE provides regulators with a specific language in which they can communicate with data controllers to

establish privacy obligations and undertake prioritized capacity building for resource-deprived data controllers.

This methodology is not just an operational guide but also a rigorous tool of critique. Under PE, compliance to PbD is not binary, but a nuanced question based on relevancy of each strategy, and its extent of operationalization through the interconnected elements of the web. Thus, there is always scope for improvement.

When compared, Account Aggregators supersedes the Aarogya Setu application in terms of every strategy and tactic. The Account Aggregator framework exceptionally embodies PbD. The strategies of "minimize", "hide", and "separate" are largely operationalized, while "abstract" is irrelevant. Some improvements are nevertheless required: a pod to fully operationalize the "destroy" tactic and mix networks for the "dissociate" tactic. The strategies of "inform", "control", 'enforce' and "demonstrate" are presently operationalized to near perfection, barring additions to the "update" tactic.

The Aarogya Setu application averagely embodies PbD. All tactics of "minimize" largely find compliance. Under "hide", the standard of documentation needs to be higher to "restrict" while "obfuscation" of unique IDs and 'dissociation' of distinct datasets through mix networks needs to be done. AS' unique architectural design operationalizes "separate" to the greatest possible extent. However, data can be better "abstracted" by operationalizing the "perturb" and "summarize" tactic through differential privacy and dynamic location granularity. AS 'informs' well using simple and accessible explainer. However, full operationalization requires privacy issues to be condensed into one document and prompter notifications. While users' "control" their "consent", this control can be improved through real-time alerts as to the processing of their data and security breaches. While the bounty program and grievance officer are welcomed, required clarifications and scope extensions are

needed. To fully "enforce" privacy compliance, AS' team must make four-fold changes to make its open source fully meaningful. Lastly, "demonstrate" is better operationalized by logging organizational decisions, extending scope and transparency of current audits, and improving frequency of responses to public concerns.

The evaluation of these technological solutions through PE reveals the manner in which the relevancy question must be resolved, and the application of relevant factors to determine the extent to which the web must be operationalized for achieving the minimum amount of data protection. Ultimately, the satisfactory compliance by both these technological solutions indicates that PbD has already permeated into India's techno-legal regime. It is now important that this approach finds not only global affirmation but also greater global application.