

## **ELP Discussion Paper:**

Justice BN Srikrishna Committee -  
White Paper on Data Protection

---

## Table of Contents

<i>Preface</i> .....	3
<i>Introduction</i> .....	4
Justice AP Shah Report .....	4
Supreme Court in Puttaswamy .....	4
TRAI Consultation Paper .....	5
Justice BN Srikrishna Committee .....	5
<i>What Type of Data Needs Protection?</i> .....	7
‘Personal Data’ and ‘Sensitive Personal Data’ .....	7
Exemptions to Companies from Data Protection Laws .....	8
‘Pseudonymised Data’ and ‘Anonymised Data’ .....	8
<i>Data Controllers and Data Processors</i> .....	9
Definitions .....	9
Who should be Responsible for Data Protection? .....	9
<i>Consent</i> .....	10
Issues .....	10
Proposed Method of Seeking Consent: Notice .....	11
Individual’s Rights over Past Data .....	12
Grounds for Processing of Personal Data without Consent .....	12
A Child’s Consent .....	12
<i>The Government</i> .....	13
The Government as Data Controller .....	13
Exceptions to Government from Data Protection Laws .....	13
<i>Monitoring and Enforcement</i> .....	14
Enforcement Framework: Co-Regulation .....	14
Enforcement Mechanism .....	15
Remedies .....	16
<i>Cross-Border Flow of Information and Data Localisation</i> .....	17
Jurisdictional Issues with Cross-Border Flow of Information .....	17
Enforcement Methods for Cross-Border Offences .....	17
Data Localisation .....	17

## Preface

Dear Reader:

Data privacy is a burning issue. After the landmark decision of the Hon'ble Supreme Court in *Puttuswamy*<sup>1</sup> the government has appointed a committee under the chairmanship of Justice B.N. Srikrishna. The Srikrishna Committee released a white paper raising several critical issues.

With a view towards highlighting the issues and enhancing the debate, ELP has prepared this Alert. Prior to this we had prepared a background and analysis of the privacy debate in ([available here](#))

We do hope you will find this analysis useful and will use this opportunity to share your views on this important issue – both for you personally and your organization.

As always we welcome your feedback so do drop us an email at [MehfuzMollah@elp-in.com](mailto:MehfuzMollah@elp-in.com) or [SuhailNathani@elp-in.com](mailto:SuhailNathani@elp-in.com)

**Regards**

**Suhail Nathani**

**Managing Partner | Economic Laws Practice**

---

<sup>1</sup> Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors. 2017 (10) SCALE 1.

## Introduction

Recently the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors.*<sup>2</sup> (“*Puttaswamy*”) unanimously held that the right to privacy is a fundamental right. During the course of the hearing, based on suggestion from the Bench, the Government of India constituted a Committee under the chairmanship of Justice (Retd.) BN Srikrishna with the following terms of reference: (a) to study various issues relating to data protection in India; and (b) to make specific suggestions for consideration of the Central Government on principles to be considered for data protection in India and suggest a draft data protection bill.

Prior to the Justice Srikrishna Committee there was a committee constituted under the Chairmanship of Justice A.P. Shah in 2012. The TRAI had also floated a paper on data privacy for the telecom sector and various stakeholders have commented on that paper. Where relevant, these have been discussed in this Discussion Paper, along with the issues raised by the White Paper issued by the Justice Srikrishna Committee.

### *Justice AP Shah Report*

---

In 2012, the erstwhile Planning Commission of India had constituted a committee under the chairmanship of Justice AP Shah to deliberate and analyse the national privacy principles in the light of the emerging issues both in India and globally. The committee submitted its report on October 16, 2012 (“*Justice AP Shah Report*”).<sup>3</sup>

The framework suggested by Justice AP Shah Report was based on the following five salient features:

1. Technological neutrality and interoperability with international standards;
2. Multi-Dimensional privacy;
3. Horizontal applicability to state and non-state entities;
4. Conformity with privacy principles; and
5. A co-regulatory enforcement regime.

### *Supreme Court in Puttaswamy*

---

On August 24, 2017, a nine-judge bench of the Supreme Court of India in the landmark decision in *Puttaswamy*<sup>4</sup> unanimously ruled that the right to privacy is intrinsic to life and liberty and hence is a fundamental right under Article 21 of the Constitution of India. For a detailed discussion on the nuances of the case please refer to ***ELP Alert: Data Protection & Privacy Issues in India (September 2017)***. The major highlights of the decision is provided below:

- Privacy is intrinsic to and inseparable from human element in human being.
- Right to Privacy is not just a common law right but a fundamental right guaranteed by Part III of the Constitution.
- Privacy is not an absolute right, subject to permissible restrictions.
- Action must be sanctioned by law, it must be necessary to fulfil a legitimate aim of the State and the interference must be ‘proportionate to the need for such interference’.
- Recognition and enforcement of claims for breach qua non-state actors will require legislative intervention by the State.

---

<sup>2</sup> Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors. 2017 (10) SCALE 1.

<sup>3</sup> Accessible online at: [http://planningcommission.nic.in/reports/genrep/rep\\_privacy.pdf](http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf)

<sup>4</sup> Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors. 2017 (10) SCALE 1.

- Right to privacy was grounded in rights to freedom under both Article 21 and Article 19 of the Constitution encompassing freedom of the body as well as the mind.

During the deliberation, the Government of India informed the Supreme Court that a committee under the chairmanship of Justice (Retd.) BN Srikrishna has been constituted to analyse the global practices and recommend a suitable data protection law for India. Noting this fact the Supreme Court of India directed the Committee to frame its recommendations in light of the observations made in the instant matter.

### ***TRAI Consultation Paper***

---

Meanwhile, on August 09, 2017, the Telecom Regulatory Authority of India (“**TRAI**”) released a consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector<sup>5</sup> for stakeholders’ comments. The aim of the paper was to identify the key issues pertaining to data protection in relation to the delivery of digital services. TRAI, in its consultancy paper, had sought comments from the public on twelve separate questions – they range from the definition and ownership of the personal data to regulation and audit of data controllers to balancing of rights of each stakeholder to the issue of cross-border flow of information.

Till date TRAI has received 53 comments and 12 counter-comments from different stakeholders in the value chain. Though the consultation was open to the public at large, most comments were received from the Telecom Service Providers (“**TSP**”), over-the-top (“**OTT**”) content providers and the industry associations. We have referred to the comments whenever relevant.

### ***Justice BN Srikrishna Committee***

---

On July 31, 2017, the Government of India constituted a committee of ten experts on data and privacy laws from different domains under the chairmanship of Justice (Retd.) BN Srikrishna with a mandate to study and recommend a suitable data protection law for India. After initial deliberation the committee released a ***White Paper on Data Protection framework for India***<sup>6</sup> (“**White Paper**”) for public comments.

The White Paper has deliberated on various aspects and issues on data privacy laws across various jurisdictions around the world. The main themes as identified by the White Paper are:

1. ***Technology agnosticism-*** The law must be technology agnostic. It must be flexible to take into account changing technologies and standards of compliance.
2. ***Holistic application-*** The law must apply to both private sector entities and government. Differential obligations may be carved out in the law for certain legitimate state aims.
3. ***Informed consent-*** Consent is an expression of human autonomy. For such expression to be genuine, it must be informed and meaningful. The law must ensure that consent meets the aforementioned criteria.
4. ***Data minimisation-*** Data that is processed ought to be minimal and necessary for the purposes for which such data is sought and other compatible purposes beneficial for the data subject.

---

<sup>5</sup> Accessible online at:

[www.trai.gov.in/sites/default/files/Consultation\\_Paper%20on\\_Privacy\\_Security\\_ownership\\_of\\_data\\_090820\\_17.pdf](http://www.trai.gov.in/sites/default/files/Consultation_Paper%20on_Privacy_Security_ownership_of_data_090820_17.pdf)

<sup>6</sup> Accessible online at:

[http://meity.gov.in/writereaddata/files/white\\_paper\\_on\\_data\\_protection\\_in\\_india\\_171127\\_final\\_v2.pdf](http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf)

5. **Controller accountability-** The data controller shall be held accountable for any processing of data, whether by itself or entities with whom it may have shared the data for processing.
6. **Structured enforcement-** Enforcement of the data protection framework must be by a high-powered statutory authority with sufficient capacity. This must coexist with appropriately decentralised enforcement mechanisms.
7. **Deterrent penalties-** Penalties on wrongful processing must be adequate to ensure deterrence.

Since the purpose of the White paper was to engage with the stakeholders, the White Paper shies away from taking any final position on the issues; and the views taken are only provisional in nature. The White Paper has put across detailed and very specific questions around most of issues for the public to comment.

In this Discussion Paper we have only highlighted the provisional views of the committee.

# What Type of Data Needs Protection?

## 'Personal Data' and 'Sensitive Personal Data'

Today the main enactment that deals with protection of data is the Information Technology Act, 2000 ("IT Act") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011 (the "IT Rules").

Personal information is defined under Rule 2(i) of the IT Rules to mean "any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person".

It is noteworthy that, at present, only sensitive personal data (a sub-set of personal data) is protected under the IT Act and the IT Rules. Rule 5 of the IT Rules prescribes that **no body corporate shall collect sensitive personal data or information** unless (a) the information is collected for a lawful purpose connected with a function or activity of the body corporate; and (b) the collection of such information is considered necessary for that purpose. Rule 6 of the IT Rules prescribes that **no body corporate can disclose sensitive personal information to any third party** without permission from the provider of such information.

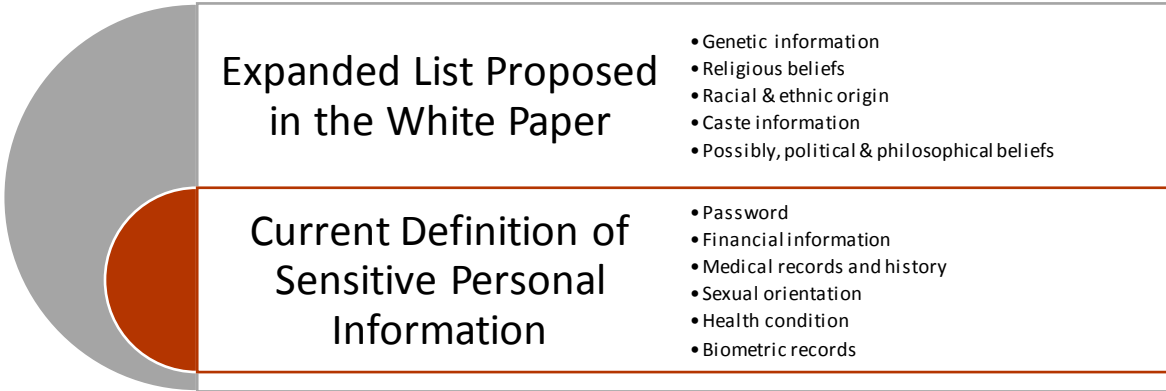
The White Paper proposes that the present definition could be expanded to include opinions and assessments irrespective of their accuracy.<sup>7</sup>

According to the White Paper, the data protection laws should provide protection to the entire gamut of personal data<sup>8</sup> with a higher level of protection to sensitive personal information than personal data<sup>9</sup> and a more stringent penalty be imposed for harm/breach of privacy law involving sensitive personal data.<sup>10</sup> The White Paper has proposed an expanded list of personal data to be categorised as sensitive (See Box 1: ).

**TRAI Stakeholder Comments**

Most of the industry players in the telecom sector (including the Industry Associations) have said that the current definition (under IT Act) is in line with the international best practices and is sufficient to cover the definition of personal data and does not require further change. MTNL, however, observes that the definition should also include data of any third persons such as phone book contacts.

**Box 1: Sensitive Personal Information**



<p><b>Expanded List Proposed in the White Paper</b></p>	<ul style="list-style-type: none"> <li>• Genetic information</li> <li>• Religious beliefs</li> <li>• Racial &amp; ethnic origin</li> <li>• Caste information</li> <li>• Possibly, political &amp; philosophical beliefs</li> </ul>
<p><b>Current Definition of Sensitive Personal Information</b></p>	<ul style="list-style-type: none"> <li>• Password</li> <li>• Financial information</li> <li>• Medical records and history</li> <li>• Sexual orientation</li> <li>• Health condition</li> <li>• Biometric records</li> </ul>

<sup>7</sup> Page 39 of the White Paper  
<sup>8</sup> Page 39 of the White Paper  
<sup>9</sup> Page 41 of the White Paper  
<sup>10</sup> Page 203 of the White Paper

## Exemptions to Companies from Data Protection Laws

At present the IT Rules provides the following two exemptions to body corporates from the application of Rule 5:

1. the information collected for a lawful purpose
2. the collection of such information is necessary for that purpose

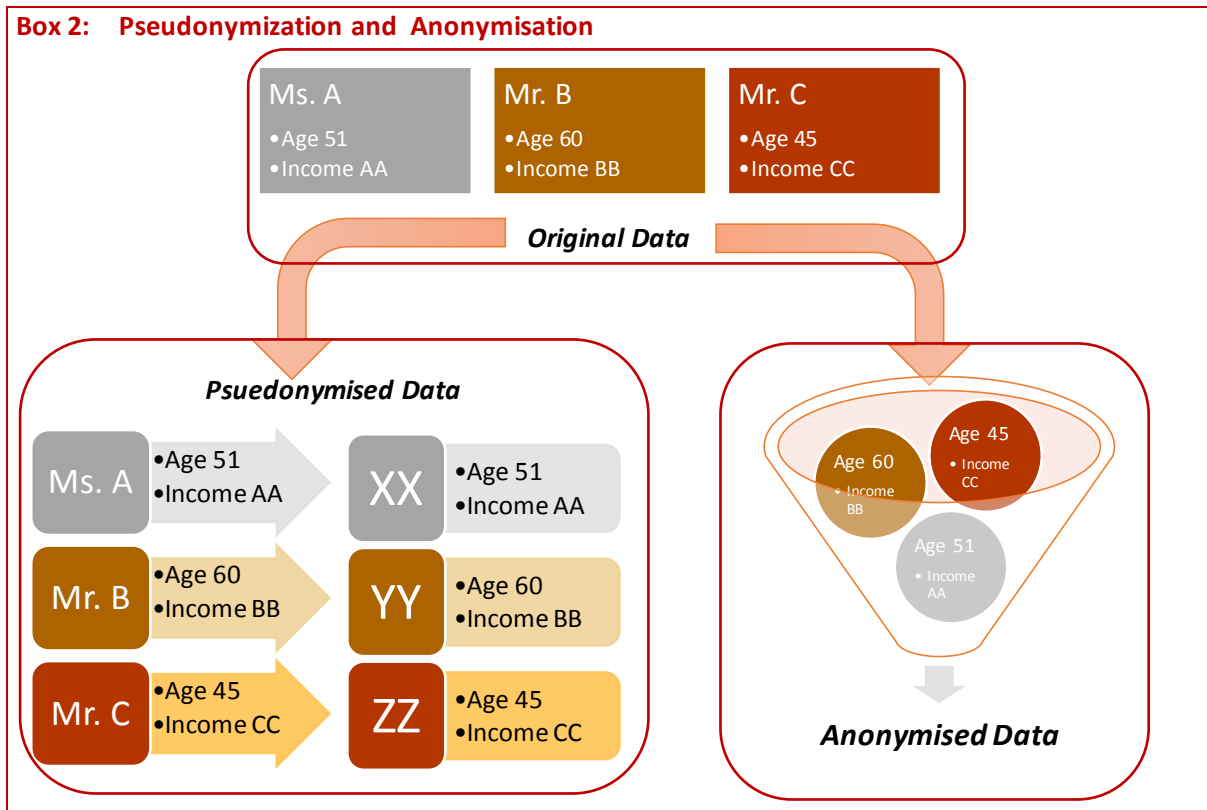
The White Paper proposes to increase the scope of the categories of information that deserves exemption from data protection laws to include household purposes (i.e. information collected for an individual’s own use), journalistic/artistic, literary, academic research, statistics and historical purposes.<sup>11</sup>

### TRAI Stakeholder Comments

Broadband India Forum was of the opinion that private data could only be shared for academics or other researchers for public value.

## ‘Pseudonymised Data’ and ‘Anonymised Data’

Anonymisation seeks to remove the identity of the individual from the data, while pseudonymisation seeks to disguise the identity of the individual from data. Anonymization irreversibly destroys any way of identifying the data subject. Pseudonymization substitutes the identity of the data subject in such a way that additional information is required to re-identify the data subject (See Box 2: ).



Globally, in most jurisdictions, anonymised data falls outside the scope of personal data while pseudonymised data continues to be personal data. The White Paper has reserved its views on this and has sought stakeholder’s comments on the same.<sup>12</sup>

<sup>11</sup> Page 59 of the White Paper

<sup>12</sup> Page 40 of the White Paper



## Data Controllers and Data Processors

### Definitions

The concepts of data controllers and data processors are not provided clearly under the IT Act or the IT Rules. The words “originator”<sup>13</sup> and “intermediary”<sup>14</sup> as defined under the IT Act are insufficient for the purpose of data protection law.

According to the White Paper, the competence to determine the purpose and means of processing may be the test for determining who is a ‘data controller’.<sup>15</sup> Whereas a data processor is an entity which is closely involved with processing, which however, acts under the authority of the data controller.<sup>16</sup>

#### TRAI Stakeholder Comments

Various stakeholders (including Idea, Internet and Mobile Association of India, Broadband India Forum, etc) were of the view that the scope and definition of data controller, data processor and data subject must be lucidly and clearly defined in the applicable laws.

### Who should be Responsible for Data Protection?

Basing its approach in lines with the EU Model,<sup>17</sup> the White Paper proposes that the data controller should be primarily responsible for compliance with data protection norms; while the data processor may be provided with some level of responsibility.<sup>18</sup>

Additionally, the White Paper suggests that based on the degrees of risks there should be some form of differentiated obligations between different kinds of processing activities undertaken by the data processors.<sup>19</sup>

#### TRAI Stakeholder Comments

Few Industrial Associations (viz: EBG Federation, Broadband India Forum & BSA – The Software Alliance) are of the view that distinguishing between data controller and data processor is important to identify who is responsible for any data breach. Some go on to further say that the data controllers should primarily be responsible for complying with the law. If anything, data processors should be responsible to take the necessary technical and organizational measures to secure the data they process on behalf of the controller. The ‘controller-processor’ relationships are governed through contractual means and the law should not unreasonably intervene in these relationships.

<sup>13</sup> Section 2(1)(za) of the IT Act states: “originator” means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary.

<sup>14</sup> Section 2(1)(w) of the IT Act states: “intermediary” with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.

<sup>15</sup> Page 50 of the White Paper

<sup>16</sup> Page 48 of the White Paper

<sup>17</sup> In the EU the applicable regulation is General Data Protection Regulations (“GDPR”); approved and adopted by European Parliament (“EU”) in April 2016 and will come into force on May 25, 2018.

<sup>18</sup> Page 50 of the White Paper

<sup>19</sup> Page 171 of the White Paper

# Consent

## Issues

The Hon'ble Supreme Court in *Puttaswamy*<sup>20</sup> held that right to privacy is a fundamental right and the same include informational privacy that recognises that an individual should have control over the use and dissemination of information that is personal to him. Since any unauthorised use of personal information would lead to an infringement of this right, his consent should be taken for collection or processing of this information.

However, there are certain issues with collection of information even with consent. The White Paper discusses the following four issues:

### 1. *Lack of Meaningful and Informed Consent*

The most popular mean of seeking consent is through notice to the user by the organisation informing the user of the potential use and dissemination of such personal information. Quite naturally it is expected that the notice would provide a fair and truthful information of the potential use of the consent. However, quite often we do not see that in practice.

### 2. *Standards of consent*

According to the White Paper there is a need to have different standards of consent (and information in the notice) based on the sensitivity the personal data.

### 3. *Consent Fatigue*

With the rise of computing power data processing has become routine work and as a result of this the users are flooded with consent notices.

### 4. *Lack of Bargaining Power*

According to the White Paper, at present most of the online services come with only "take it or leave it" option. There is no provision for negotiation and the user has to forego the services offered.

### TRAI Stakeholder Comments

All stakeholders agree that user's consent for use of its personal/sensitive information is absolutely necessary. However, the method of obtaining consent could vary. According to most Industry Associations and OTT players (viz: Internet Service Providers Association of India, zeotab, Citibank, etc) the user must be given a choice of either "opt-in" or "opt-out".

According to GSM Association, Collection of consent is not always easy (and sometimes redundant because the consumers generally always agree to online consent forms) and companies can give a consumer certain control (without the need for consent) like dashboard or tools to "opt-in" or "opt-out".

However, most consumer association (eg: Consumer Protection Association) believes that if sensitive information is involved then there should be explicit consent of the user.

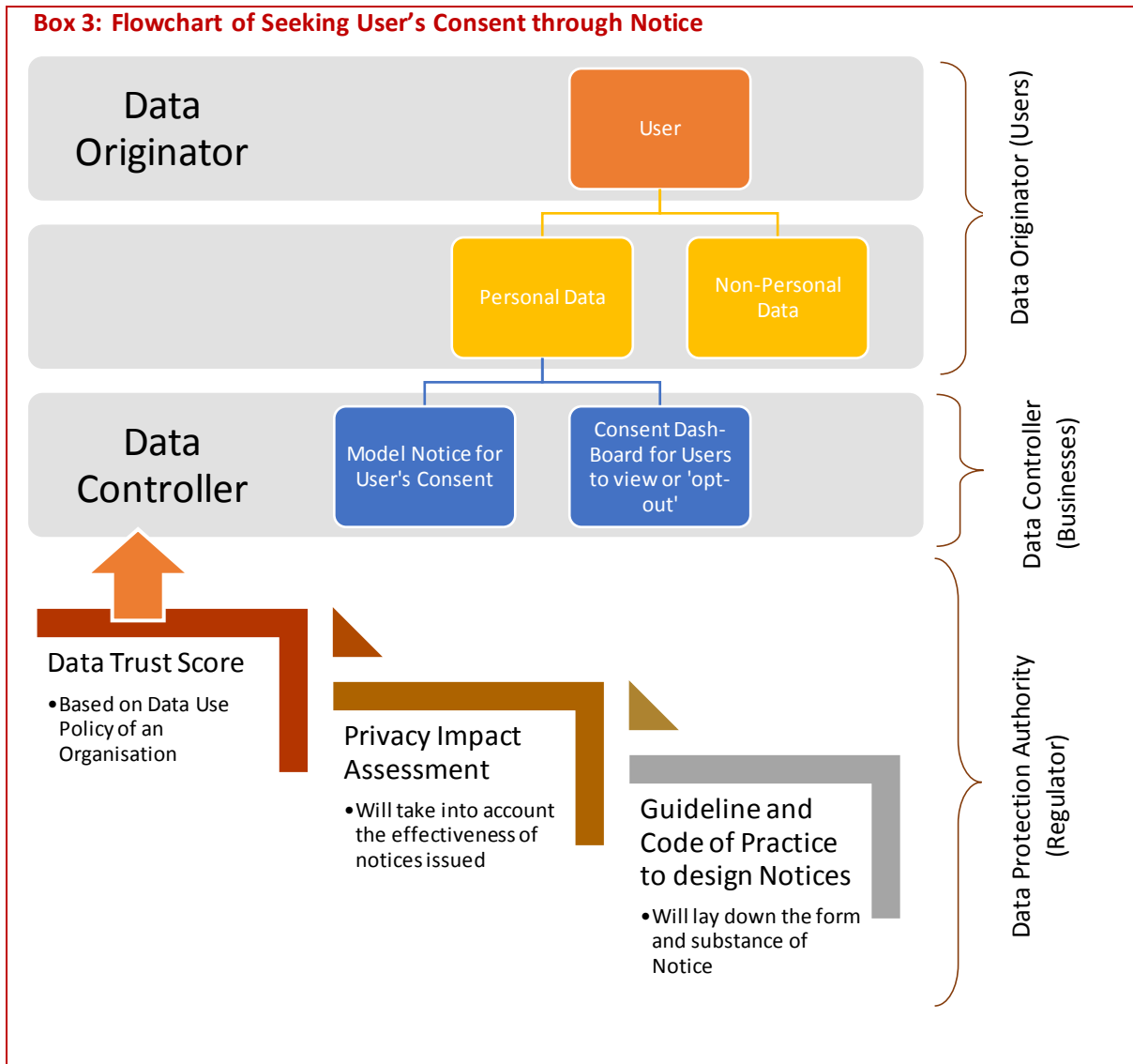
<sup>20</sup> Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCALE 1.

**Proposed Method of Seeking Consent: Notice**

The White Paper recommends the mandatory use of notice for privacy management and seeking consent of the users.<sup>21</sup> It envisages that a Data Protection Authority<sup>22</sup> would provide detailed guidelines and code of practices to regulate form and substance of the notice. The interface between the user, the data controller and the regulator is provided below.

**TRAI Stakeholder Comments**

US India Business Council (USIBC) recommends “Notice Principle” system. However, Disney prefers self-regulatory regimes rather than overly burdensome notice.



<sup>21</sup> Page 97 of the White Paper

<sup>22</sup> A regulator proposed to be formed under the data protection laws for enforcement (*discussed later*).

## Individual's Rights over Past Data

---

### Right to View and Rectify

The White Paper recognises the right of the individual to have view access and to rectify his personal data.<sup>23</sup> However, such a right may be costly for the organisations and the individual may be charged a reasonable fee for it.

### Right to be Forgotten

According to the White Paper, the right to be forgotten may be incorporated within the data protection framework.<sup>24</sup> However, such a right must be in lines with clear parameters laid down by the regulator.

### TRAI Stakeholder Comments

US India Business Council (USIBC), few of the TSPs/ Industry Association (viz. GSM Association, Cellular Operators Association of India and Bharti Airtel) are of the view that companies should respect the customer's right to be forgotten and respect the customer's request to delete her personal data at the termination of service (bearing in mind that anonymous data is not personal data).

### Portability of Data

The White Paper proposes to include the concept of data portability into the data protection law.<sup>25</sup> A corollary to this is that all data must be held in an interoperable format.

## Grounds for Processing of Personal Data without Consent

---

According to the White Paper, *consent and notice* may not be the only ground of processing of personal data; and when processing is routine then obtaining consent prior to every such transaction may lead to consent fatigue.<sup>26</sup> The White Paper has suggested the following situations when prior consent is not required:<sup>27</sup>

1. Performance of contract
2. Compliance with law
3. Collection of information in situations of emergency
4. Other "legitimate interest" – the Data Protection Authority can designate certain activities as lawful and provide guidelines for data controllers for these grounds

### A Child's Consent

---

According to the White Paper, children should be accorded higher standard of protection; and as such parental authorisation or consent would be required for data controllers to process personal data relating to children.<sup>28</sup>

The White Paper further proposes that a variable age limit (the threshold being lower than 18) could be considered below which parental consent would be required.

### TRAI Stakeholder Comments

According to the Consumer Protection Association, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only to the extent that consent by the holder of parental responsibility.

---

<sup>23</sup> Page 127 of the White Paper

<sup>24</sup> Page 141 of the White Paper

<sup>25</sup> Page 135 of the White Paper

<sup>26</sup> Page 99 of the White Paper

<sup>27</sup> Page 103 of the White Paper

<sup>28</sup> Page 89 of the White Paper

## The Government

### *The Government as Data Controller*

---

According to the White Paper, the law should apply horizontally to data about natural persons processed both by public and private entities. However, limited exemptions may be considered for well-defined categories of public or private sector entities.<sup>29</sup>

### *Exceptions to Government from Data Protection Laws*

---

The Hon'ble Supreme Court in *Puttaswamy*<sup>30</sup> has laid down a threefold requirement for State's interference with the fundamental rights. While the State may intervene to protect legitimate state interests:

- (a) there must be a law in existence to justify an encroachment on privacy, which is an express requirement of Article 21 of the Constitution,
- (b) the nature and content of the law which imposes the restriction must fall within the zone of reasonableness mandated by Article 14, and
- (c) the means which are adopted by the legislature must be proportional to the object and needs sought to be fulfilled by the law.

The White Paper has taken this into consideration and has proposed exemptions for the following information:<sup>31</sup>

1. Information necessary for the purpose of investigation of a crime, and apprehension or prosecution of offenders;
2. Information necessary for the purpose of maintaining national security and public order.

In addition, the White Paper proposes a review mechanism to ensure that this exemption is not granted unreasonably.

---

<sup>29</sup> Page 32 of the White Paper

<sup>30</sup> *Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors.* 2017 (10) SCALE 1.

<sup>31</sup> Page 59 of the White Paper

# Monitoring and Enforcement

## Enforcement Framework: Co-Regulation

The White Paper proposes a co-regulation model of enforcement.<sup>32</sup> Co-regulation form of enforcement may be described as initiatives in which government and industry share responsibility for drafting and enforcing regulatory standards. Basic features of co-regulation model of enforcement are:

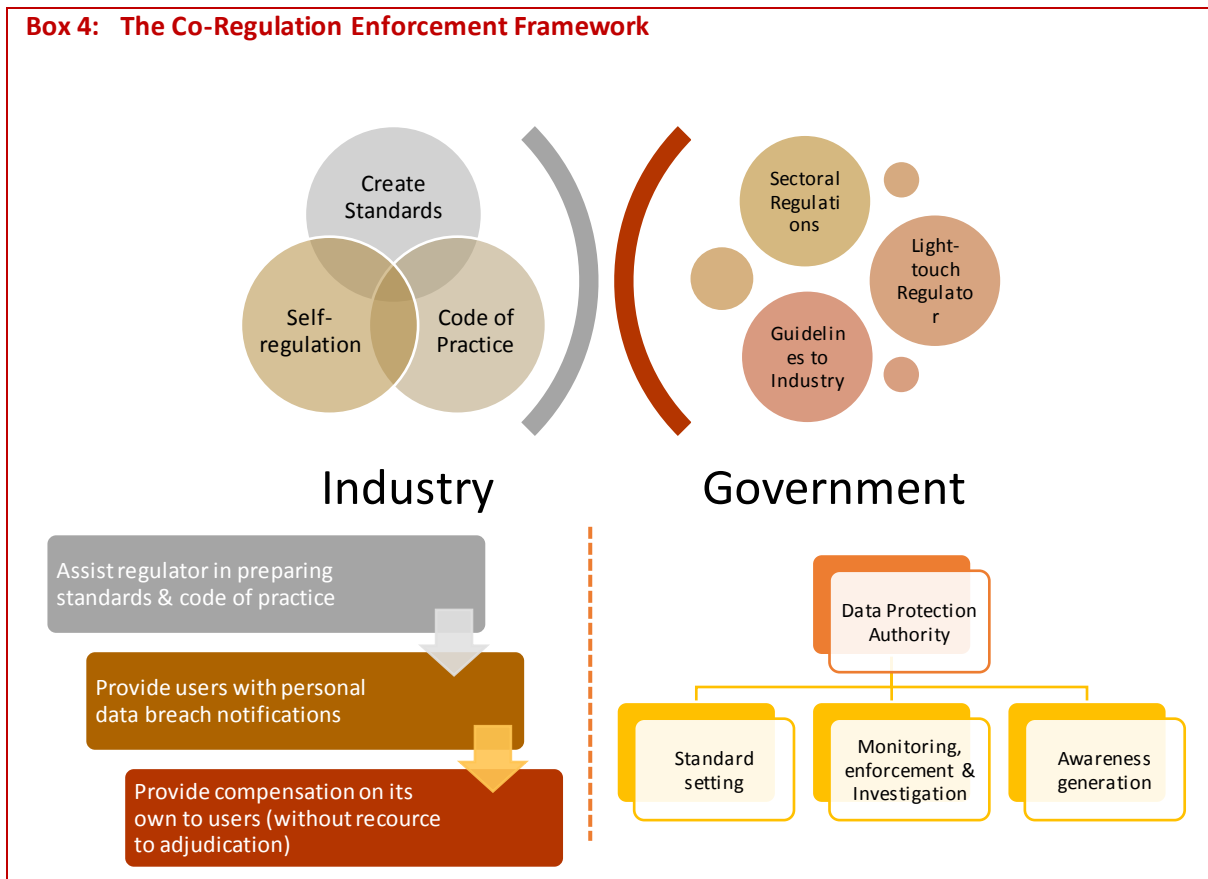
1. Formation of a general data protection statutes with broad provisions (eg: Industry Codes of Conduct)
2. Compliance with the detailed provisions of the Codes of Conduct would be indication of compliance with general provisions of the statutes

### TRAI Stakeholder Comments

Most Industry Associations (viz: GSM Association and Cellular Operators Association of India) are of the opinion that the best way to regulate data controllers is through laying down of broad principles and encourage them to have internal compliances; and accountability should be reflected in all businesses.

Since the issues pertaining to data protection is highly specialised the White Paper proposes to setup a separate and independent **data protection authority** at the national level with powers to (i) monitor, enforce & investigate; (ii) generate awareness; and (iii) setting of standards.<sup>33</sup> The interface between the Industry and Government in a co-regulation model along with the role of the Industry and the Government is presented a schematic format below:

**Box 4: The Co-Regulation Enforcement Framework**



<sup>32</sup> Page 146 of the White Paper

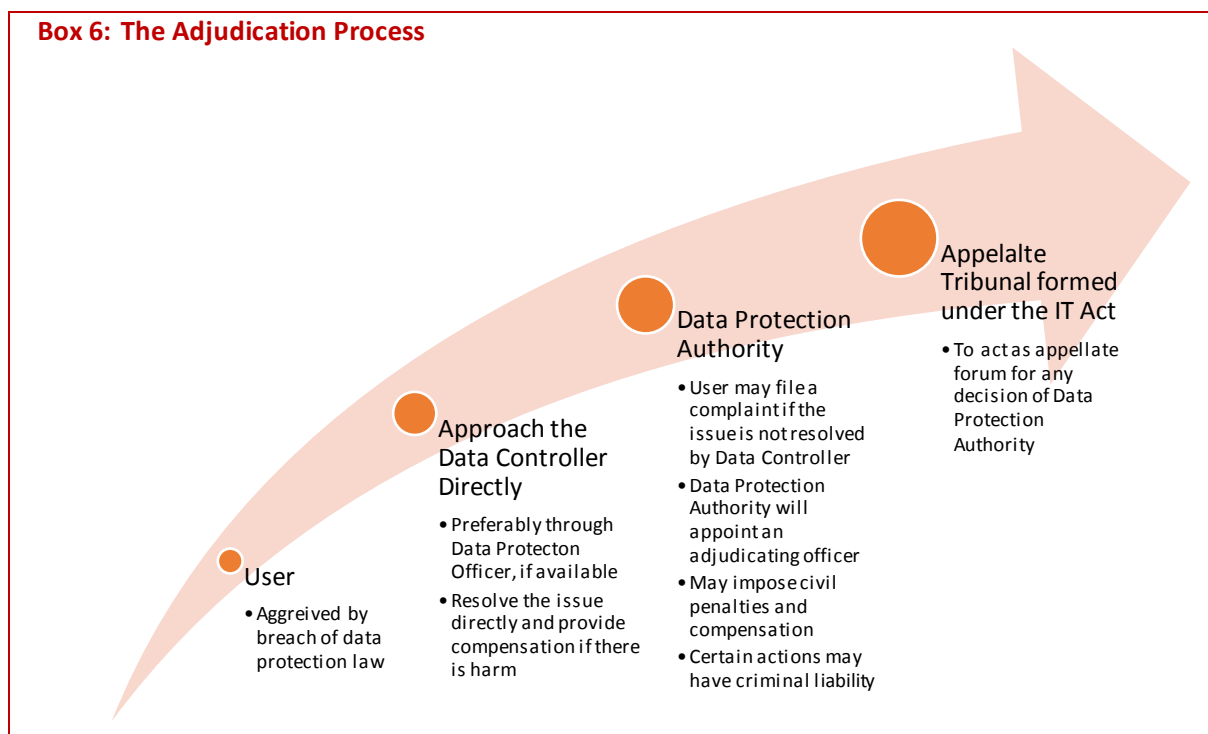
<sup>33</sup> Page 181 of the White Paper

The White Paper has suggested some form of differentiated obligations for data controllers involved in activities which has higher degree of risk.<sup>34</sup> In the following table the additional obligations for data controllers are discussed:

Box 5: Additional Responsibilities for Certain Data Controllers			
<p style="text-align: center;">Registration</p> <ul style="list-style-type: none"> <li>•Applicable to only certain Data Controllers (as determined by the Regulator)</li> </ul>	<p style="text-align: center;">Data Protection Impact Assessment</p> <ul style="list-style-type: none"> <li>•Applicable only to specific Data Controllers (eg: new technology or risky activities)</li> </ul>	<p style="text-align: center;">Data Audits</p> <ul style="list-style-type: none"> <li>•Regular Audits through independent auditing agencies</li> <li>•Applicable only to Data Controllers with high risk activities</li> </ul>	<p style="text-align: center;">Data Protection Officer</p> <ul style="list-style-type: none"> <li>•Designated individual within organisation</li> <li>•Advisory role</li> <li>•Interface with users for grievance redressal</li> </ul>

### Enforcement Mechanism

The White Paper has provided some detailed observations with respect to the adjudication process and has noted that the present adjudication framework is inadequate.<sup>35</sup> The main feature of the proposed framework is that the aggrieved individual should approach the data controller first before approaching the Data Protection Authority. The White Paper also suggests that some actions would incur criminal liability; and where the investigation would be undertaken at a decentralised level (i.e. by a police officer not below the rank of Inspector).<sup>36</sup> The adjudication process is presented below:



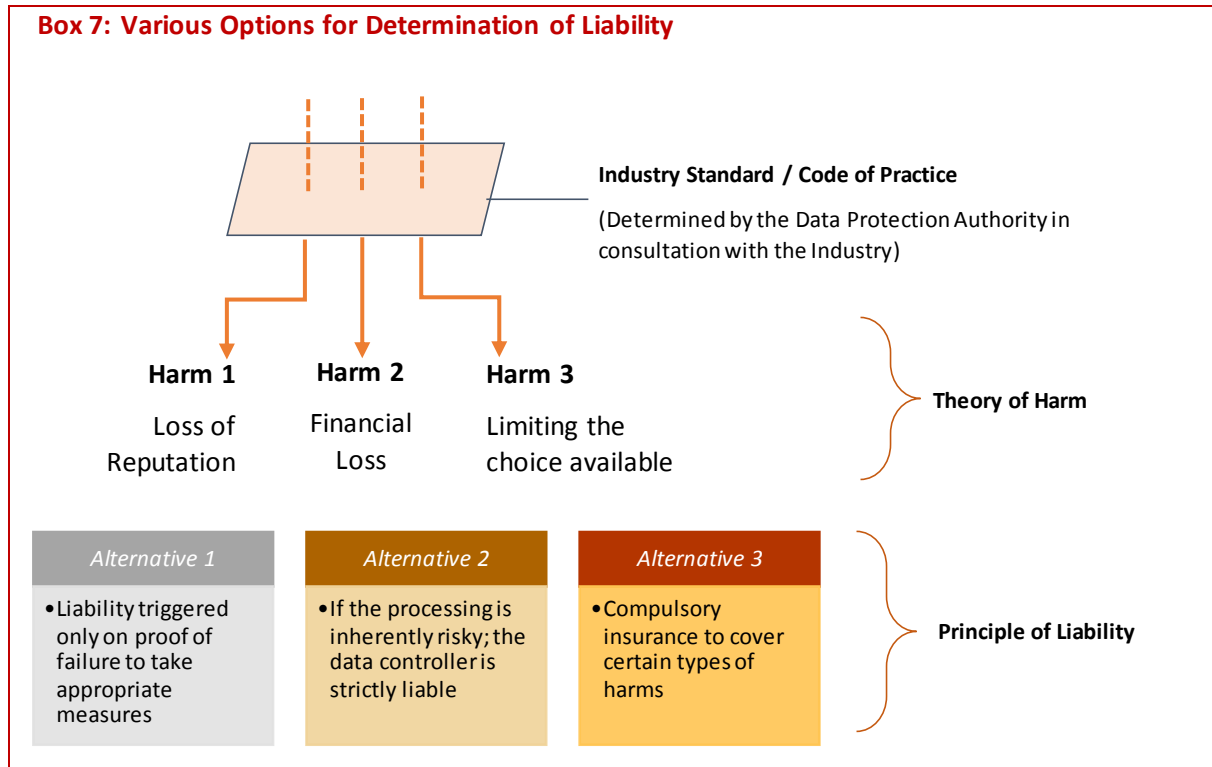
<sup>34</sup> Page 171 of the White Paper

<sup>35</sup> Page 188 of the White Paper

<sup>36</sup> Page 203 of the White Paper

## Remedies

While discussing the principles of harm and liability the White Paper identifies three types of harm to the user.<sup>37</sup> In the following scheme the proposed theory of harm is explained with the possible alternatives for allocating liability.



<sup>37</sup> Page 149 of the White Paper



## Cross-Border Flow of Information and Data Localisation

### *Jurisdictional Issues with Cross-Border Flow of Information*

---

The ease at which data can flow across jurisdictional border is both a matter of advantage and disadvantage. The fact that foreign entities need not establish local office for its operations would mean substantial lowering of operational cost which could then be passed on to the consumers. On the other hand, it might be difficult to implement sanctions on these foreign firms because they are outside the jurisdictions of Indian laws. In the absence of any treaty or agreement cross-border implementation or enforcement of sanctions in most matters is generally guided by the principles of comity.<sup>38</sup> However, the same does not provide legal certainty.

The White Paper proposes that all entities, even which does not have a presence in India, that offers a good or service to Indian residents over the Internet, or carries on business in India may be covered under the law.<sup>39</sup> Additionally, in lines with EU GDPR, the White Paper proposes that any entity (no matter where they are located) that processes the personal data of Indian citizen or resident should be covered under the data protection law.<sup>40</sup>

### *Enforcement Methods for Cross-Border Offences*

---

As discussed above, there are some issues with enforcement of sanctions. In order to address this issue the White Paper has suggested the following enforcement techniques:<sup>41</sup>

1. Mutual legal assistance treaties
2. Restriction of access to the market
3. Adopt penalties based on global turnover
4. Mandatory establishment of a representative office; and holding Indian subsidiary/ related entities liable for damages

### *Data Localisation*

---

Data localisation mandate companies to store and process data on servers physically located in national borders.

The White Paper is of the view that only a few countries have adopted data localisation in some form or the other. It is of the opinion that while data localisation may be considered in certain sensitive sectors, it may not be advisable to prescribe it across the board.<sup>42</sup>

---

<sup>38</sup> Black's Law Dictionary 2004 (8<sup>th</sup> Edition) defines comity as "A practice among political entities (as nations, states, or courts of different jurisdictions), involving esp. mutual recognition of legislative, executive, and judicial acts. "'Comity,' in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive, or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens, or of other persons who are under the protection of its laws." *Hilton v. Guyot*, 159 U.S. 113, 163–64, 16 S.Ct. 139, 143 (1895).

<sup>39</sup> Page 28 of the White Paper

<sup>40</sup> Page 28 of the White Paper

<sup>41</sup> Page 27 of the White Paper

<sup>42</sup> Page 75 of the White Paper