To,
Justice Srikrishna Committee of Experts on Data Protection
C/O Shri Rakesh Maheshwari,
Scientist G & Group Co-ordinator, Cyber Laws
Ministry of Electronics and Information Technology (MeitY)
Electronics Niketan, 6, CGO Complex,
Lodhi Road, New Delhi - 110003

Dated : Jan. 31, 2018

Submission by legal academics and advocates to the Justice Srikrishna Committee of Experts on Data Protection

> "As *nightfall does not come all at once, neither does oppression. In both instances, there is a twilight where everything remains seemingly unchanged. And it is in such twilight that we must all be most aware of change in the air - however slight - lest we become unwitting victims of the darkness*"
>
> > William O. Douglas, Letter to the Washington State Bar Association, 1976. [As quoted by Arvind Datar, Senior Advocate during oral submissions before the Hon'ble Supreme Court in the case of, Binoy Viswam v. Union of India (2017) 7 SCC 59]

Dear sir,

We are writing to you as a collection of practising lawyers and policy professionals having experience in public policy debates on law and technology. The leitmotif of our submission is the proposal for a citizen centric data protection law that protects and extends our fundamental rights to the intersection of law and technology. To aid greater awareness and participation in this consultation exercise we are proactively publishing our response to the committee. We hope that the submission will not only be considered by the Committee but will also be freely shared, copied and extracted by individuals and organisations to aid in spreading awareness on the issues involved.

Our responses are divided into three primary sections. The first section contains several procedural recommendations to the committee, followed by a summary of key comprehensive substantive recommendations in the second section, and more detailed context to the substantive recommendations in the third section. In addition to our submission to the committee we have published this document online on www.privacyisaright.in under the Creative Commons BY 2.5 IN license (link).

An alphabetically sorted list of signatories is given below:

Anup Surendranath	Apar Gupta	Chinmay Kanojia	Gautam Bhatia
Jawahar Raja	Karan Lahiri	Kotla Harshvardhan	Kritika Bhardwaj
Mariyam Kamil	Maansi Verma	Mihira Sood	Ninni Susan Thomas
Paras Nath Singh	Prasanna S.	Raghav Shankar	Rahul Narayan
Raman Jit Singh Chima	Sai Vinod	Shadan Farasat	Suhrith Parthasarathy
Tanvi NS	Ujwala Uppaluri	Vrinda Bhandari	Saurabh Bhattacharjee

I. Increase diversity, participation and transparency

We are writing to you as a collection of practising lawyers and policy professionals having experience in public policy debates on law and technology. The leitmotif of our submission is the proposal for a citizen centric data protection law that protects and extends our fundamental rights to the intersection of law and technology. To aid greater awareness and participation in this consultation exercise we are proactively publishing our response to the committee. We hope that this submission will not only be considered by the Committee but will also be freely shared, copied and extracted by individuals and organisations to aid in spreading awareness on the issues involved.

Our second concern arises from the structure of the present consultation exercise which has the effect of dulling and de-incentivising public participation. This shortfall is evident from the framing of the white paper's contents. Regrettably, individual aspects of a data protection statute have been presented with granular, microscopic level of detail without, at the same time, substantively setting out the big picture on data protection. The white paper principally contains a comparative summary of foreign legislations that spread over two hundred and thirty one pages and poses two hundred and thirty three questions for public comment. We respectfully submit that the sheer breadth and complexity could have easily been reduced by first conducting a public consultation limited to the key principles of a data protection legislation. While the white paper does contain a summary and lists key principles in Part V, it is disappointing that these same principles have not been reasoned within the text of the preceding portions and also do not fit expressly with the provisional views of the white paper.

We also have further concerns, which arise from the electronic participation mechanism designed by MeitY, in which persons are expected to respond to the two hundred thirty

three questions in individual form fields on MyGov.in. Answering two hundred and thirty three questions is manually exhausting and unnecessarily arduous. This approach will limit participation to well resourced organisations with full-time employees focused on such tasks, and disproportionately increase the representation of commercial and private industry players to the detriment of the representation of other stakeholders and the wider spectrum of Indian citizenry. We hope that wide public participation across a diverse group of persons and entities enriches the present consultative exercise, as noticed during the SaveTheInternet.in (STI) campaign on Net Neutrality.

The third and final concern relates to a lack of transparency. The National Campaign for People's Right to Information (NCPRI) has written to this committee about the denial of its right to information request seeking information on the proceedings of the committee, meeting notes and a draft bill which has been forwarded by MeitY [link]. We urge the committee to adopt greater transparency and release this information as well as publish the comments received by it to enable counter comments by the public.

We, therefore, request three key changes in the conduct of the present consultation exercise to build public confidence in the eventual recommendations of the committee :

1) **Increase diversity :** Co-opt members of academics, members of civil society, technologists and experts who hold views independent or even critical of Aadhaar, to improve the diversity of the committee. Preference may be accorded to women and those from marginalised sections of India's population.

2) **Invite public participation :** Publish an official and public summary of the white paper and invite public comment on the primary principles, limited to a set of 10 key questions. To make the participation process inclusive a summary document could be published in English, Hindi and other widely spoken regional languages.

3) **Improve transparency :** Pro-actively release all information about the appointment, constitution, functioning and working of the committee in the public domain including meeting and agenda notes, file notings, materials which are being considered by it, particularly the draft data protection statute forwarded by the MeitY. Release all comments made to the committee as they constitute public records.

II. Summary of substantive recommendations

To effectively deliver on the constitutional promises articulated by the Supreme Court's judgement on the right to privacy, we suggest:

Recommendation No. 1 : Individual rights are at the center of privacy and data protection

We, therefore, submit that the Committee's Draft Data Protection law should be based upon the following constitutional axioms:

(1) That the individual is an end in herself.

(2) That individual autonomy, dignity, and self-determination (as articulated by *Puttaswamy*) constitute the heart and soul of the Indian Constitution.

(3) That the Data Protection Law must not articulate and tackle the central problem as achieving an acceptable trade-off between "innovation" and "data protection", but as achieving a legislative and regulatory framework which harnesses innovation in order to facilitate individual autonomy, dignity, and self-determination.

Recommendation No. 2 : Adopt a principle based approach

(1) Adopt the core principles of privacy and data protection as articulated by the report of the Justice A.P. Shah Committee of Experts [link];

(2) Incorporate subsequent developments including the Puttaswamy decision and the European Union's General Data Protection Regulation.

(3) Exceptions should remain exceptions and should not swallow up the rule. Any exceptions to the privacy principles should be: (a) exceptions brought about through a clearly worded legal instrument, (b) narrowly tailored exceptions that proceed from an analysis of the necessity of the exemption, (c) the necessity and proportionality of these exemptions (in their creation and practical operation) must be closely connected to the aim for which they are created; and (d) exceptions must be accompanied by sufficient procedural safeguards for the preservation of individuals' rights and of accountability to the regulator.

Recommendation No. 3 : Create an empowered, independent regulator to enforce the privacy principles

In keeping with our submissions, we suggest the following structure for the office of a privacy commissioner:

(1) The privacy principles adopted in the legislation should be implemented by a strong and independent privacy commissioner having wide powers of investigation, rule-making and enforcement.

(2) The law should provide for the creation of a Privacy Commission, at the Central and State levels, that is well funded, well staffed and transparent in its appointment process. The composition of a Privacy Commission should include sector experts and civil society, and have sufficient safeguards for independence from government interference in its functioning.

(3) The Privacy Commission at the Central Level should have binding rule making powers over the government and the private sector through which to develop the privacy principles into regulations as technology and its use changes with time. All regulations should be formed by robust public consultation processes. This allows the Privacy Commission to be responsive to technological advances and ensures the fulfillment of the intent of the enactment.

(4) To ensure effective enforcement, the Privacy Commission should have powers of investigation, adjudication and enforcement. These include the power to impose penalties in the nature of fines and also the power to file criminal complaints for wilful non-compliance of the rules and regulations made by the Privacy Commission to build deterrence.

(5) Data harms are tangible and serious and hence generalised arguments of forbearance, "regulatory sandboxes" or "light touch regulation" are inapplicable to a Privacy Commission. Market based mechanisms (educational, capacity building) and incentives to promote the implementation of privacy law by design should not be a substitute or tradeoff for enforcement, binding rules or penalties.

Recommendation No. 4 : Aadhaar conflicts with privacy protections and any version of a citizen centric data protection law

(1) The recommendations of the committee should examine the Aadhaar Unique ID project in its full ambit, including its practical execution and its purported legality — as arising from the Aadhaar Act, 2016 — to enable changes to core features of the project and the Act that are incompatible with a data protection statute.

(2) We support the use of digital technologies for public benefit. However, they should not be privileged over fundamental rights. Any digital identity scheme should be framed around the protection of individual rights through a data protection

legislation, rather than a data protection legislation being framed to presumptively accommodate and work around an existing program such as Aadhaar.

(3) The following core features of the Aadhaar program are incompatible with the privacy principles:

(a) Compulsion in enrollment and authentication. This negates principles of consent, choice and self-determination. We suggest that the scheme should be made purely voluntary and existing Aadhaar users should be provided with an opt-out.;

(b) Reliance on biometrics as a method of enrollment and authentication. This negates human dignity, and fails the tests of necessity and proportionality and the other requirements enunciated in the principles. All biometric data should be deleted and a complete shift should be made to other forms of authentication such as OTPs;

(c) Universal reliance on the Aadhaar scheme by both the Central and State Governments, and especially by the private sector. This dissolves the silos in which data is held, enables pervasive profiling by allowing a unique identifier to be linked across databases and violates purpose limitation. Separate schemes and digital identities should be implemented after viability studies that may be linked to digital keychains or management systems which work without pulling in meta-data and authentication logs across services.

(d) Absence of data breach notifications and credible remedies for individuals against the UIDAI. This violates the principle of accountability. Amendments are urgently necessary within the Aadhaar Act to address this concern.

(4) The Privacy Commission should have overriding power and superintendence over the UIDAI. The UIDAI being a data controller and a data protection authority for Aadhaar data at the same time - as currently set out by the Aadhaar Act - creates a conflict of interest.

Recommendation No. 5 : *An effective, citizen friendly adjudicatory system*

(1) Members of the public, in instances of disputes or allegations of violation of data protection regulations, should have the ability to make complaints to the Privacy Commission.

(a) Individual and class complaints should ordinarily be made to the State Privacy Commissions.

(b) A class of affected persons (not necessarily a legal entity such as an association or registered body), or a representative action by an individual should be made directly to the Central Privacy Commission.

(c) Privacy Commissions should have the ability to investigate (independently through the office of a Director General), hold hearings and pass orders with directions and fines.

(d) Privacy Commissions should also be empowered to file criminal complaints in the course of acting on complaints made to them.

(2) Appellate review over directions and fines should be put in place to ensure deterrence. The statute should also require a pre-deposit of a percentage of the monetary fine prior to filing an appeal. Such statutory condition is necessary to factor in a period of pendency at the stage of appeals and enable compliance during this period.

(a) Statutory appeals from orders of the State Commissions should be appealable to the Privacy Commission.

(b) Orders of the Privacy Commission should have finality. They should be made statutorily appealable to the Supreme Court of India on the restricted grounds of the existence of a substantial question of law or an error apparent on the face of record.

(3) In addition to complaints to the Privacy Commission, persons should retain the remedies of approaching the civil courts (even in instances where harm is suffered by a group of people) and of filing police complaints directly. We caution against the creation of any new adjudicatory tribunals or conferring exclusive jurisdiction on existing ones as it is likely to create barriers to access to justice for the general public.

Recommendation No. 6 : A comprehensive data protection law is incomplete without surveillance reform

(1) State security and intelligence agencies which intercept and record personal communications and data require statutory recognition. At the very least, they need to be brought within a system of parliamentary oversight. The existing regime, which involves intelligence agencies established under colonial administrative orders, is incompatible with *Puttaswamy* as well as with any citizen focused data protection law.

(2) Mass or, "dragnet" surveillance -- which is unrestricted surveillance directed over a group or class of persons should be prohibited in principle as contravening the principles of necessity, proportionality and purpose limitation.

(3) Procedural safeguards for surveillance and interception orders need to be strengthened as the existing ones are inoperational and deficient. We recommend several safeguards including prior judicial scrutiny in which public defenders are appointed on behalf of the proposed subject of surveillance as well as notification of the existence and content of such orders to the subject of surveillance when it ceases.

(4) We further recommend amendments to the Indian Evidence Act whereby evidence which is gathered illegally, such as telephone intercepts without valid tapping orders, are made inadmissible. This would be in line with the judgment of the Hon'ble Supreme Court in *Selvi vs State*.

Recommendation 7: *The right to public information needs to be strengthened and protected*

(1) Individual rights are well served by the Right to Information Act which brings accountability to the functioning of government and public authorities. Hence, privacy protections which already exist under the Right to Information Act are made subject to public interest, need to be preserved. Accordingly, the Right to Information Act should not be subjected to any change by this committee.

(2) Specific and express language should be used exempting Information Commissioners from interference or control by the Privacy Commissioner and maintaining their independence.

(3) The "right to be forgotten" or the right to de-indexing from search engines may undermine the fundamental right to free expression and should be developed within the framework of the privacy principles by the Privacy Commissioner rather than being expressly present in the statute. Given the journalistic and public interest in the maintenance of public information, sufficient safeguards need to be adopted.

Recommendation 8: *International harmonisation that recognises cross-border data flows to protect the open internet*

(1) Any data protection regulation must have extra-territorial effect and apply to web services and platforms which are accessible in India and which gather personal data of Indians. To ensure compliance, the Privacy Commission should also be empowered to confer adequacy status, in a transparent process, to foreign countries from which such global platforms carry out their operations.

(2) At the same time, care and caution should be taken to preserve the global character of the open internet which is beneficial to Indians as they can access

information, knowledge and services from all over the world. Hence, any suggestions, such as blanket data localisation proposals, which would threaten and undermine the global open internet need to be resisted.

(3) In the age of a global, open internet, our data protection framework must protect the data of our citizens globally and focus on interoperability.

III. Reasoning and context to our recommendations

Recommendation No. 1 : Individual rights are at the center of privacy and data protection

> "*That the individual shall not be required to relinquish any of his constitutional rights as a condition precedent to the receipt of a privilege.*"
>
> B.R. Ambedkar, States and Minorities (1947)

> "*Privacy is a part of personhood and is therefore a natural right. This why the natural right is not conferred but only recognised by the Constitution*"
>
> Gopal Subramanium, Senior Advocate in his written submissions before the Hon'ble Supreme Court in *Justice KS Puttaswamy (Retd.) & Anr. v. Union of India & Ors* [W.P. (C) 494/2012]]

On 24th August 2017, a nine-judge bench of the Supreme Court of India handed down a landmark judgment in *Justice K.S. Puttaswamy vs Union of India* (2017) 10 SCC 1. Not only did *Puttaswamy* affirm the existence of the fundamental right to privacy under the Indian Constitution, but it also reminded us of how the Constitution articulates the relationship between the individual and the State, and the role of fundamental rights in characterising and mediating this relationship.

Central to the six concurring opinions in *Puttaswamy* was the understanding that the individual is at the heart of the Constitution. The Constitution exists to protect individual autonomy, dignity, and self-determination. The fundamental rights chapter defends, advances, and fulfills these constitutional values by recognising and affirming a set of inalienable rights. It does this not only by erecting a wall between the individual and the State, and prohibiting the State from breaching that wall (except in certain limited circumstances), but also by imposing positive obligations upon the State to ensure that fundamental rights become an effective reality for every Indian. We believe that the central feature of any data protection law should be to check the power of the State and preserve the fundamental rights of the individual.

The judgment in *Puttaswamy* accomplished this by articulating a rich and substantive vision of privacy, located not only in Article 21's guarantee of a right to life and personal liberty, but also within other crucial fundamental rights, such as the rights to freedom of speech (19(1)(a)), association (19(1)(c)), movement (19(1)(d)), and conscience (25). Privacy, according to the Court, has two dimensions. Privacy, in its negative dimension, protects constitutional values of dignity, autonomy and self-determination by prohibiting the State from infringing upon certain sacrosanct domains, such as private spaces, private relationships, and intimate decisions and choices. By creating these domains of sanctity, linked to the individual, the Supreme Court understood privacy as a tool to remedy the unequal power relationships that exist between the individual and the State, and to protect the individual from being in a position of dependence, or subservience, to the State.

In doing so, the Court drew upon a rich Indian intellectual tradition, closely linked to our freedom struggle. It was in the early twentieth century that Mahatma Gandhi had understood how open infringement of privacy - and the collection of information about individuals - served as a method of State control and dominance. Gandhi's campaign against the compulsory fingerprinting of Indian males in the South African province of Transvaal was based upon the fundamental insight that information can be a source of power, and an imbalance of power between State and individual can become a source of dominance and dependence - a concern that is a golden thread running through the six separate opinions in *Puttaswamy*. We believe that a similar, vast and unhindered power is being formalised through the Aadhaar program.

The second dimension of privacy, as the Court held in *Puttaswamy*, is a positive dimension. Privacy, in its positive sense, advances and fulfills constitutional values by requiring the State to take positive action by creating a legal framework that will allow individuals to realise these values in their daily existence. It is to advance this positive dimension of privacy that the Justice Srikrishna Committee, tasked with formulating a data protection law, has come into being - a fact recognised by the Supreme Court itself in *Puttaswamy*. We applaud this move, and we seek to support and strengthen the work of the Committee in formulating an effective data protection act by offering substantive feedback on the Committee's White Paper.

We also appreciate the complexity of the task facing the Committee: while fulfilling its positive obligations by creating a legal framework dealing with the regulation of individual data and information, the State must be careful not to distribute or allocate powers in a manner that may infringe the right to privacy in its negative dimension. In other words, a data protection law must provide a framework that regulates data in a manner that individuals are able to effectively exercise their rights to substantive autonomy and self-determination - and at the same time, it must ensure that those who have the power to control or process data are not put in positions where such powers can be used to dominate individuals, or reduce them to a situation of dependency.

Therefore, while we endorse and agree with many of the White Paper's recommendations (***see below***), for the reasons advanced above, we take issue with the overarching framing of the White Paper. In the Foreword to the Paper, the second sentence reads as follows:

> "*The objective* [of the data protection law] *is to —ensure growth of the digital economy while keeping personal data of citizens secure and protected.*"

We respectfully disagree. We dispute assertions that personal data is oil or that people are natural resources to be exploited for commercial profit and experiment. We believe that this framing is based on the assumption that a data protection law must enact a balance between the "growth of the digital economy" and "keeping personal data of citizens secure and protected" - that is, it envisions a trade-off between the goals of economic growth and data protection. We believe that this presents a false choice, because the "*growth of the digital economy*" is not - and cannot be - an *end in itself*. On the contrary, both the digital economy and security of personal data are instrumental in achieving the same set of constitutional goals: protecting and fulfilling individual autonomy, dignity, and self-determination. Such objectives are subcomponents of citizen interests rather than than a competing claim for their limitation.

Our comments and responses to the White Paper, therefore, are articulated within this framework, and in furtherance of B.R. Ambedkar's important insight about the role of fundamental rights in a constitutional democracy. In his notes accompanying the clauses of a draft Bill of Rights, Ambedkar noted that:

> "*The purpose is to protect the liberty of the individual from invasion by other individuals which is the object of enacting fundamental rights. The connection between individual liberty and the shape and form of the economic structure of society may not be apparent to everyone. Nonetheless the connection between the two is real. It will be apparent if the following considerations are borne in mind.*
> *Political democracy rests on four premises which may be set out in the following terms:*
> *The individual is an end in himself.*
> *That the individual has certain inalienable rights which must be guaranteed to him by the Constitution.*
> *That the individual shall not be required to relinquish any of his constitutional rights as a condition precedent to the receipt of a privilege.*
> *That the State shall not delegate powers to private persons to govern others.*"

In the Constituent Assembly Debates, Ambedkar would go on to affirm that "*the… Constitution… has adopted the individual… as its unit*."

We, therefore, submit that the Committee's Draft Data Protection law should be based upon the following constitutional axioms:

(1) **That the individual is an end in itself**
(2) **That individual autonomy, dignity, and self-determination (as articulated by *Puttaswamy*) constitute the heart and soul of the Indian Constitution**
(3) **That the Privacy and Data Protection Law must not articulate and tackle the central problem as achieving an acceptable trade-off between "innovation" and "data protection", but as achieving a legislative and regulatory framework which harnesses innovation in order to facilitate individual autonomy, dignity, and self-determination.**

We believe that there exists a rich institutional memory that this Committee can draw upon to instantiate these values. One of these is the Report of the Group of Experts on Privacy, chaired by Justice A.P. Shah, acknowledged by the White Paper in its overview of the history of data protection efforts in India. The principles articulated by the A.P. Shah Committee - especially the tests of necessity and proportionality to determine the validity of infringements on privacy - found the support of a majority of judges in *Puttaswamy*, and we shall be addressing some of these issues in our next recommendation.

Recommendation No. 2 : Adopt a principle based approach

> "*Scientists and technologists have, because of their power, an especially heavy responsibility, one that is not be sloughed off behind a facade of slogans such as that of technological inevitability. In a world in which man increasingly meets only himself, and then only in the form of the products he has made, the makers and designers of these product — the buildings, airplanes, foodstuffs, bombs and so on — need to have the most profound awareness that their products are, after all, the result of human choices.*"
>
> Joseph Weizenbaum, Computer Power and Human Reason: From Judgment To Calculation (1976)

On August 25, 2017 Indian newspapers carried headlines stating "Privacy Supreme" (the Indian Express), "SC gives India a private life" (the Times of India) and, "Historic Verdict: Right to Privacy Key to Life and Liberty" (the Hindustan Times). These headlines, coming a day after the Right to Privacy judgement, were a celebration of individual autonomy. In our opinion, the public expectations, expressed through these headlines, are best fulfilled by drawing benefit from past expert attempts to formulate privacy principles as contained in the Report of the Justice A.P. Shah Committee of Experts.

We submit that this report is an influential text for the formulation of any data protection legislation as it places the individual at the center when stating that, "*the fundamental philosophy underlying the principles is the need to hold the data controller accountable for the*

collection, processing and use to which the data is put thereby ensuring that the privacy of the data subject is guaranteed" [at Pg. 4]. We would also submit that the opinion of Justice Sanjay Kishan Kaul in this privacy judgement [at Para 74, pg. 40] makes express reference to this report. Subsequent and comparative texts including the European Union's General Data Protection Regulation as noted by the white paper provide greater guidance to make our data protection statute protective of individual rights while responsive to rapid technological change.

The Justice A.P. Shah Report report has five salient features that are summarised in the beginning, notably, (1) technological neutrality and interoperability with international standards; (2) multi-dimensional privacy, which exists in multiple contexts; (3) horizontal applicability to both government and the private sector; (4) conformity with nine privacy principles; and (5) a co-regulatory enforcement regime. We particularly lay emphasis on the nine privacy principles for adoption; however before proceeding to them we must underscore that subject matter of privacy protection in a statute must be wide and appreciate the contextuality of the harm.

Context in the design of privacy protections is especially important as, (a) categories of data which may be fairly innocuous in isolation, such as name, age, gender etc., can nevertheless, in different contexts, lead to harm; and (b) big data sets of anonymous and pseudonymous data, through reprocessing. can lead to identification and harm. Such dangers have been alerted by Dannah Boyd and Kate Crawford [link] when they recounted that:

> "*In 2006, a Harvard-based research group started gathering the profiles of 1,700 college-based Facebook users to study how their interests and friendships changed over time (Lewis et al. 2008). These supposedly anonymous data were released to the world, allowing other researchers to explore and analyze them. What other researchers quickly discovered was that it was possible to deanonymize parts of the data set: compromising the privacy of students, none of whom were aware their data were being collected (Zimmer 2008).*"

Hence, we recommend a principle based approach to define the applicability of the statute to any information or data which can lead to the identification of an individual, directly or indirectly. The statute should further recognise that a heightened form of protection may be necessary for classes of information which can lead to identification of conditions physical (genetic), mental, sexual, social (caste, language, ethnicity), political, and can cause serious harm. While we commend the white paper in its provisional views by which it states, "*[d]ata from which an individual is identified or identifiable/reasonably identifiable may be considered to be personal data. The identifiability can be direct or indirect*" [at page 39], we caution against exclusion for data sets which are claimed to be anonymised but may be identifiable by combination with other data sets. We urge that pseudonymised data

may in any instance not be excluded from the ambit of protections that are premised on the privacy principles.

An important component of the Puttaswamy Judgement was the wide ambit of the right as illustrated in the judgement when in the Order of the Court it noted, "*(iii) the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution*". This is further noticed in Chapter I of the Justice A.P. Shah Committee Report on Privacy, which notes that constitutional basis for privacy by court cases related to state surveillance, medical information and sexual identity. This is set out in Chapter II of the Report which contain nine privacy principles made applicable over, "*the collection, processing, storage, retention, access, disclosure, destruction, and anonymisation of sensitive personal information, personal identifiable information, sharing, transfer, and identifiable information*". In our submission all such activities are components of, "data processing" as queried by the White Paper in Part II, Chapter 5.

We support the provisional views of the white paper which state that, "*the definition of procession may be broadly worded to to include existing operations while leaving room to incorporate new operations by way of interpretation*"; however we are concerned that limiting them to "*collection, use and disclosure*" may limit such intent [Pg. 46]. The approach of the whitepaper by itself presumes the application of a principle based approach. To aid the formulation as to what constitutes, "*data processing*" we recommend a comprehensive ambit for the application of activities to which the privacy principles are made applicable, drawing reference to Prof. Daniel Solove's taxonomy of privacy, where he principally categorises data harms [link] as:

1. **Information collection:** Surveillance, Interrogation
2. **Information Processing:** Aggregation, Identification, Insecurity, Secondary Use, Exclusion
3. **Information Dissemination:** Breach of confidentiality, Disclosure, Exposure, Increased Accessibility, Blackmail, Appropriation, Distortion
4. **Invasion:** Intrusion, Decisional Interference.

Such harms are best evaluated against the nine privacy principles as articulated by the Justice A.P. Shah Committee Report. These principles have been distilled in the report on the basis of comparative practices that are evaluated from legislations in the United States, European Union, and the OECD and APEC guidelines. These are contained in Chapter 3 and reflect, "*a set of globally accepted privacy principles*" which are listed below for convenience:

1. **Notice :** "A *data controller shall give simple-to-understand notice of its information practices to all individuals, in clear and concise language, before any personal information is collected from them*" [Page 21]. It is reasoned that, "*The notice*

principle ensures that individuals are informed of how their information will be used, allows data controllers to communicate their intents and practices to data subjects and other stakeholders, and allows the individual to hold the data controller accountable to the practices articulated in the notice."

2. **Consent and choice:** "A *data controller shall give individuals choices (opt-in/opt-out) with regard to providing their personal information, and take individual consent only after providing notice of its information practices. Only after consent has been taken will the data controller collect, process, use, or disclose such information to third parties, except in the case of authorized agencies*" [Page 22]. It is further reasoned that, "*The principle ensures that data controllers provide simple choices to data subjects that allow them to make informed decisions about the extent to which they would like to share their personal information, prior to collecting that information.*".

   We may indicate here that there exist some misconceived attempts to argue that notice, choice and consent are ineffective privacy principles and instead priority should be given to forms of accountability. Such an understanding proceeds from a faulty understanding of privacy and data protection legislations that proceed from a basis of complementarity rather than competition of values. Hence, the importance of notice, choice, and consent remain vital to any data protection regulation. As noted by the Justice Shah Committee itself, "As mentioned in the notice principle, user centric principles such as choice and consent principles should not be used to transfer organisation's privacy obligations to data subjects, instead the organisation should take responsibility for protecting privacy" [Page 23]. Hence the privacy by design principle needs to be a pervasive, genuine, and deep implementation at the heart of each processing action and should not be reductively wished away merely by implementations of technical/digital, "consent layers".

3. **Collection Limitation :** "A data controller shall only collect personal information from data subjects as is necessary for the purposes identified for such collection, regarding which notice has been provided and consent of the individual taken. Such collection shall be through lawful and fair means." [Page 24] We would urge that this include the concept of, "data minimisation" which has been indicated within the report when it notes, " intended to minimize the data subjects' personal information dealt with by organisations by limiting collection and retention".

4. **Purpose limitation :** "A data controller shall collect, process, disclose, make available, or otherwise use personal information only for the purposes as stated in the notice after taking consent of individuals. If there is a change of purpose, this must be notified to the individual. After personal information has been used in accordance with the identified purpose it should be destroyed as per the identified procedures." [Page 24]

5. **Access and Correction :** "The access and correction principle ensures that data controllers provide access mechanisms to data subjects for inquiring if a data controller is holding their personal data, and for viewing, modifying and deleting their personal information." [Page 25]

6. **Disclosure of Information** : "The disclosure to third parties principle ensures that data subjects are informed and consent taken [except when an exemption exists] when their personal information is transferred to third parties. The principle requires data controllers ensure that third parties also adhere to the National Privacy Principles. The principle also ensures that any disclosure by the data controller to a third party that has been authorized and is a governmental agency is in compliance with the National Privacy Principles. Furthermore the principle makes any de-anonymization of information that was anonymised/aggregate information for the transfer a violation of the principle." [Page 25]

7. **Security:** "The security principle ensures that data controllers put in place the necessary technical, administrative, and physical safeguards for protecting personal information in their custody from unauthorised use, destruction, modification, access, and retention etc. – both from insiders and outsiders." [Page 26]

8. **Openness:** "The openness principle ensures that data controllers make their privacy policies, practices, systems, and related developments open, transparent, and accessible to individuals through mechanisms such as providing information in multiple languages, and adopting an open standards/accessible format for the disabled." [Page 26]

9. **Accountability:** "The data controller shall be accountable for complying with measures which give effect to the privacy principles. Such measures should include mechanisms to implement privacy policies; including tools, training, and education; external and internal audits, and requiring organizations or overseeing bodies extend all necessary support to the Privacy Commissioner and comply with the specific and general orders of the Privacy Commissioner." [Page 27]

Any exceptions to these principles should be permitted only when four distinct criteria are satisfied to ensure that exceptions remain exceptions and do not end up swallowing the rule. Such limitations are expressly suggested in the obiter of Justice S.K. Kaul in the Puttaswamy Judgement when he states them to be, "principle of proportionality and legitimacy" [Para 71].

> "The concerns expressed on behalf of the petitioners arising from the possibility of the State infringing the right to privacy can be met by the test suggested for limiting the discretion of the State: "(i) The action must be sanctioned by law; (ii) The proposed action must be necessary in a democratic society for a legitimate aim; (iii)

> The extent of such interference must be proportionate to the need for such interference; (iv) There must be procedural guarantees against abuse of such interference."

We suggest such tests may be adopted as exceptions to the privacy principles.

We make the following specific recommendations for the adoption of a principle based approach by the committee:

> **(1) Adopt the core principles of privacy and data protection as articulated by the report of the Justice A.P. Shah Committee of Experts;**
>
> **(2) Incorporate subsequent developments including the Puttaswamy decision and the European Union's General Data Protection Regulation.**
>
> **(3) Exceptions should remain exceptions and should not swallow up the rule. Any exceptions to the privacy principles should be through, (a) the existence of a legal instrument, (b) narrowly tailored exceptions that proceed from an analysis of the necessity of the exemption, (c) the necessity and proportionality of the exemption (in its creation and its practical operation) to the aim for which it was created; and (d) sufficient procedural safeguards for individuals and the regulator to preserve accountability.**

Recommendation No. 3 : Create an empowered, independent regulator to enforce the privacy principles

> "*Regulation is a response to market failure. How anyone could ever conceive of the notion that self-regulation, that is, market discipline and spontaneous collective action by (some of) the market participants, could correct this market failure is a mystery….In the financial sector and elsewhere, self-regulation stands in relation to regulation the way self-importance stands in relation to importance and self-righteousness to righteousness. It just isn't the same thing at all.*"
>
> Willem Buiter, Lessons from the global financial crisis for regulators and supervisors (2009)

On February 8, 2016, the TRAI Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016 were published in the Gazette of India [link]. These regulations prohibited, "zero rating" plans in which telecom companies could discount data usage for websites and distort the choice for internet users. The regulations marked the culmination of a grassroots public campaign which lasted for year, and which had a positive outcome

due to the principle based regulation and independent exercise of power of the Telecom Regulatory Authority of India. In the explanatory memorandum which accompanied these regulations there are several hints at both the power derived from the Telecom Regulatory Authority of India Act, 1997, the license agreements and the Telecommunications Tariff Order, 1999.

At the same time the TRAI was guided by principles not only within the statute, or regulations, but by an embrace of constitutionalism. After noting the cases of *Secretary, Ministry of Information and Broadcasting v. Cricket Association of Bengal*, (1995) 2 SCC 161 and *Indian Express Newspapers (Bombay) Put. Ltd. v. Union of India*, (1985) 1 SCC 641 the explanatory memorandum laid out its rationale clearly by stating that, "*The Authority is of the view that use of internet should be in such a manner that it advances the free speech rights of the citizens, by ensuring plurality and diversity of views, opinions, and ideas.*" We recommend a similar approach in which an empowered regulator acts on the privacy principles set out in legislation that lead it to a path of protecting individuals. This will bring distinct advantages of the regulator being future ready given the rapid adaptation of technology. It is for this reason it is important to define privacy principles and empower an independent regulator to issue regulations at a point in future, without necessarily being limited by present understandings.

In recent decades there has been a growing movement of de-regulation as tacitly noticed by the white paper, where it poses three models of regulation. The first is the model of self-regulation (akin to a laissez-faire). We outrightly reject any attempts to adopt wide self-regulatory measures given the real and grave harms to individual privacy.

Arguments for self-regulation have little evidence and basis to support claims that there is a trade-off between economic growth and strong, effective regulatory standards. Similar studies in foreign jurisdictions have evidenced little or no impact of regulatory standards on innovation. For instance data regulation in the European Union, which is often criticised for being stringent, has on the contrary been stated to, "induce firms to innovate in order to find more cost-effective ways to comply." [link]. Similarly in a response to the question, "Is regulation always an obstacle to innovation?" the authors of a study on EU regulation, state, ""The economic literature (starting from the seminal work of Ashford and later with the socalled "Porter hypothesis") has long recognised that regulation can be a powerful stimulus to innovation and entrepreneurship. The ultimate impact of regulation on innovation is an empirical, case-by-case question, and depends on the balance between innovation-inducing factors and innovation-constraining ones including compliance costs generated by regulation." [link] Given the absence of any specific data or empirical proof on the of competitiveness or innovation and on the contrary the existence of clear breaches of privacy and harm to individuals, a self-regulatory model may be avoided.

We would also caution against any attempts to create exceptions for self-regulation through, "regulatory sandboxes". As stated in of the recent papers at the LSE's Center for

Analysis of Risk and Regulation, "A 'sandbox' to encourage limited trial and error processes needs to be placed in the context of national and EU provisions. Encouraging 'sandboxes' is about maintaining regulatory standards, not about reducing regulation or 'deregulation'." [link].

The other two models suggested by the white paper include, command and control (similar to conventional structures of regulatory control) and the third is posed as, co-regulation (which has been stated to have elements of both). The provisional views of the white paper seem to adopt a co-regulatory approach. The problem with a co-regulatory approach is that it can have several meanings, which can have a significant impact on the future of privacy enforcement and regulation by the Privacy Commissioner. We would caution against the artificial reasonability and appeal of a co-regulatory approach as, "an appropriate middle path that combines the flexibility of self-regulation with the rigour of government rulemaking."

Instead we adopt and *in extenso* quote Prof. Graham Greenleaf's submission to this committee [link]:

> *"Despite its theoretical attractions (including to the AP Shah Committee), co-regulation models have had little successful take-up anywhere in the world. They are of no significance in Asian data privacy laws. 29 Co-regulatory schemes have been tried and discontinued under Australia's Privacy Act 1988, which attempted to make them a major aspect of its regulatory approach.30 The White Paper conspicuously fails to cite a single example of a successful co-regulatory scheme (pp. 144-146; pp. 157-159). The White Paper also sets up false dichotomies in attempting to find virtues in co-regulation. 'Flexibility' through industry-specific codes has no inherent relationship to co-regulation, and can be more easily achieved via a DPA's power to issue (and revoke) delegated legislation following industry consultations (see 2A below re industry codes). 'Command and control' regulatory mechanisms (ie a DPA making rules) is not inherently more technologically laggard, nor slow-moving, than some industry-based committee. It just has fewer vested interests. There is a risk everywhere that 'data security' and other industry bodies would like to get their hands on regulation-making powers concerning privacy. Calls for co-regulation are too often a disguised call for self-regulation, which have a proven history of failure. 31 Despite the White Paper's half-hearted attempt to endorse co-regulation, the rest of Part IV proceeds to then avoid it, indicating that it is a sop to a minority of committee members."*

We are avoiding comment on the specific enforcement rules such as codes of practice, audit, privacy officers and the need for differentiated requirements. In our assessment a statute should focus on the creation of an independent regulator and provide guidance on principal leaving the regulatory toolkit to the discretion of the regulator.

In keeping with our submissions we suggest the following structure for the establishment of a Privacy Commission:

(1) The privacy principles adopted in the legislation should be implemented by a strong independent privacy commissioner having wide powers over persons for investigation, rulemaking and enforcement.

(2) The law should provide for the creation of a Privacy Commission, at the Union and State level, that is well funded, well staffed and transparent in its appointment process. The composition of a Privacy Commission should promote the inclusion of sector experts and civil society and have sufficient safeguards for independence from government interference in its functioning.

(3) The Privacy Commission at the Union level should have binding rule making powers over the government and the private sector to develop the privacy principles into regulations as technology and its use changes with time. All regulations should be formed by robust public consultation processes. This provides several benefits where regulations can be responsive to technological advances and ensure fulfillment of the intent of the enactment.

(4) To ensure the enforcement of the regulations made by the Privacy Commission should have powers of investigation, adjudication and enforcement. These include the power to place penalties in the nature of fines and also file criminal complaints for wilful non-compliance of the privacy principles that are operationalised through rules and regulations made by the Privacy Commission to build deterrence.

(5) Data harms are tangible and serious and hence generalised arguments of forbearance, "regulatory sandboxes" or "light touch regulation" are inapplicable to a Privacy Commission. Market based mechanisms (educational, capacity building) and incentives to promote the implementation of privacy law by design should not be a substitute or tradeoff for enforcement, binding rules or penalties.

Recommendation No. 4 : Aadhaar conflicts with privacy protections and any citizen centric data protection law

> *The Committee are also unhappy to observe that the UID scheme lacks clarity on many issues such as even the basic purpose of issuing "aadhaar" number. Although the scheme claims that obtaining aadhaar number is voluntary, an apprehension is found to have developed in the minds of people that in future, services / benefits including food entitlements would be denied in case they do not have aadhaar number…*

> 42nd Report of the Standing Committee on Finance, Lok Sabha Secretariat (December, 2011) [Para 5, Recommendations]

> *Through the Finance Bill, [Finance Minister] Jaitley also expanded the use of Aadhaar, the government's biometric identification system, making it mandatory for every individual to provide their Aadhaar number while filing tax returns. Since not paying tax is a punishable crime, the government, effectively, compelled every citizen to obtain an Aadhaar number. The Biju Janata Dal leader Bhartruhari Mahtab confronted Jaitley over the issue in the Lok Sabha during the debate on the Finance Bill, saying, "you are forcing the citizens" to get Aadhaar numbers. "Yes we are," Jaitley replied.*

> Atul Dev, Balancing Act (The Caravan, June 2017)

On July 22, 2015 the Attorney General during the hearing of the case titled as *Justice K.S. Puttaswamy (Retd.) v. Union of India* [W.P. (C) 494/2012] made an argument disputing the fundamental right to privacy under Part III of the Constitution by pointing to inconsistency in precedent. This came during the midst of final arguments and required a reference by an Order dated August 11, 2015. This case was a constitutional challenge to the Aadhaar scheme prior to the passage of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 as a money bill on March 25, 2016. This context is important as not only it illustrates that the objections on grounds of individual privacy and data protection emerge from the legality of the Aadhaar scheme (that would be restricted to the Aadhaar Act), but it's very conceptualising, and core features of its practical operation.

Even the architects and proponents of the scheme lend support to a comprehensive review when they state, "*given India still doesn't have a single, well-defined law that regulates data privacy, such concerns are valid. The UIDAI was well aware of these issues, and hence designed all of Aadhaar's data collection, storage and retrieval processes with great emphasis on security. These design decisions have been outlined in great detail in many of the technical documents put out by the UIDAI*" [Nandan Nilekani & Viral Shah, Rebooting India 18 (2015)]. Repeated disclosures of data breaches, biometric replay attacks and centralisation of data and its use by private entities draw greater focus not only on the protections in law, but the deficiencies in the technical architecture and safeguards of Aadhaar. Hence, the review of the Aadhaar scheme (its architecture, process and security policies) in itself is an urgent necessity by involving a wide, transparent review by independent technologists and researchers given the composition of the committee which has a heavy representation of professionals who have worked for, or voiced support for the Aadhaar scheme in public.

We would also urge the Aadhaar scheme to be given adequate prominence in the recommendations of this committee. Aadhaar is not merely an incidental program for

digital identities, but has been made mandatory for a whole range of public and private services. It is a core element of the policies of the Government as illustrated by the speech of the Hon'ble Prime Minister at the recently concluded Global Conference on Cyber Space [link]:

> "*I am sure most of you are already aware of Aadhaar, which is the unique biometric identity of a person. We have used this identity to liberate our people from queues and cumbersome processes. Three factors: first, financial inclusion through our Jan-Dhan bank accounts; second, the Aadhaar platform; and third, the Mobile phone, have greatly helped reduce corruption. We call this the J.A.M. or JAM trinity. Through better targeting of subsidies, the JAM trinity has prevented leakages to the tune of nearly 10 billion dollars so far.*"

Aadhaar's ubiquity and indiscriminate use have even been noticed in the right to privacy judgement when it stated, "*During the course of the hearing of these proceedings, the Union government has placed on the record an Office Memorandum dated 31 July 2017 by which it has constituted a committee chaired by Justice B N Srikrishna, former Judge of the Supreme Court of India to review inter alia data protection norms in the country and to make its recommendations.*" [Chandrachud J., at Para 185]. We submit that a holistic, comprehensive review of the Aadhaar Scheme is necessary. Hence the recommendations of the committee should examine the Aadhaar project in its full ambit of practical execution, as well as it's purported legality -- as arising from the Aadhaar Act, 2016, to enable changes to its core features that are incompatible with a data protection statute.

We support the use of digital technologies for public benefit; however, they should not be privileged over fundamental rights. The context and the existence of the present consultation arises from the Aadhaar scheme which today has become a technical apparatus built off the compulsory use of biometrics. Rather than limiting the mandate of the Committee to recommend changes merely to the Aadhaar Act, 2016 which may provide some safeguards through legislative amendment, a substantive holistic appraisal of the scheme itself is necessary. It is our submission that such an examination of Aadhaar as a scheme demonstrates its inherent coercion for enrollment and lack of consent.

Some salient features of the **lack of consent and notice** during enrollment and authentication are given below:

(a) Between 2010-2016 when the Aadhaar project was operational without any legislative backing, residents were made to part with personal demographic and biometric information without any counselling or information provided during the enrolment process. Hence, there was an absence of notice and consent. In this respect the enrollment of persons was done on the back of extensive district level campaigning by private enrollment agencies who

received a fee for each enrollment without adequate government supervision of a facility for counselling of the residents.

(b) Even after the legislation of the Aadhaar Act, the Aadhaar project continues to violate informed consent, as there is an absence of choice for enrollment. Enrollment requires individuals to part with demographic and biometric information to private enrolling agencies as a necessary precondition to avail subsidies, benefits and government services [Sections 2(1) and 3 of the Aadhaar Act and the Aadhaar (Enrolment and Update) Regulations, 2016].

(c) Beyond enrollment, Aadhaar has been made mandatory as a method of authentication without providing an option to the citizen to use any other equivalent or alternative mode of identification. This violates the principle of informational self-determination and further undermines choice and consent. [Section 7 and 8 of the Aadhaar Act].

(d) Such compulsion is not limited to the Aadhaar Act but the scheme itself under which close to 150 government schemes and a number of private companies require Aadhaar data and use it for authentication. The Aadhaar scheme also operates through independent enactments and departmental circulars which include bank linking (Prevention of Money Laundering Maintenance of Records Second Amendment Rules, 2017), mobile linking (Department of Telecom circular) and PAN linking (Section 139AA Income Tax Act, 1961). Hence, the mandatory nature of Aadhaar which has personal data for enrollment and authentication violates the consent and choice principle as a scheme by itself much beyond the Aadhaar Act.

The absence of consent during enrollment and authentication is congenital to the Aadhaar project and violates the basic principle of any privacy and data protection legislation. We would also caution against the adoption of any post-jure ratification of such illegality through a "*consent layer*" or any technical dashboard for Aadhaar users to monitor their data. As cautioned by a recent report of Privacy International titled as, "*Fintech: Privacy and Identity in the New Data-Intensive Financial Sector*" [link].

> "*First, consent cannot be seen as a panacea if opting out excludes someone from society...Second, there is the question as to whether individuals are able to read and understand the full amount of information required for them to give informed consent. In the context of the fintech industry, it becomes troubling to base so much on consent when it is being manipulated by the very apps that an individual is using....Thirdly, this operates in a context where one of the goals of the sector is to change the behaviour of individuals:... In the context of the fintech industry, it becomes troubling to base so much on consent when it is being manipulated by the very apps that an individual is using.*"

We stress on the recommendation in the Privacy International report and urge the committee to consider it when it states for, "W*hen implementing identity or authentication schemes*", that, "*make the scheme voluntary, always providing alternative identification mechanisms, not conditioning the provision of any public service to its use, and providing effective opt-out mechanisms;*". Even though many of us hold diverging personal views on the Aadhaar scheme, with some favouring its complete repeal --- at the very least there is a large consensus that it be made expressly voluntary with a provision for an opt-out to comply with principles of notice, choice and consent. We would also forewarn that against state incentives that are administratively implemented to render the exercise of such a choice moot.

The Aadhaar program has made biometrics a central feature of the enrollment and authentication process for obtaining Aadhaar and establishing identity. **Biometric enrollment and authentication negates human dignity, necessity and proportionality, access-correction and security.**

- **Compulsory parting with biometrics negate human dignity**: The Indian Supreme Court has at several occasions adopted the famous edict in *Munn v. Illionois [153 (1877) 94 U.S. 113]* to hold that right to life means more than mere animal existence, including a right to life with human dignity. Such dignity which is noted in the Puttaswamy Judgement on the right to privacy would include protecting their autonomy, a necessary component of which would be informational self-determination which is violated by the compulsion to part with biometric data. Further, the GDPR expressly segments out biometric data as a special category of personal data and prohibits the processing of "*biometric data for the purpose of uniquely identifying a natural person*" unless one of the enumerated exemptions under Article 9(2) apply. (Art. 9(1)). Hence, biometric data by itself especially is recognised as sensitive personal data which should not be ordinarily parted as it conflicts with human dignity. As illustrated below even the stated purposes for which such biometric data has been parted have not been met out and they result in a gross denial of privacy, data protection and human rights.

- **Biometrics are superfluous to digital identification, thereby violating necessity and proportionality:**

    - *Biometrics is disproportionate data gathering since they are unique identifiers:* Biometrics are stated to be unique identifiers and hence can be potentially used to link data in several databases. This is further confirmed by the actual use requirement to link Aadhaar with different government registrations for availing services. This constitutes an incredibly powerful and deeply pervasive master key to the government which is unwarranted to its stated use of preventing leakages in subsidies or government benefits. Further as

evidenced by its more recent use for everything from tax evasion, money laundering, terrorism to even airport check-ins, there is an incredible amount of function creep, making the choice of biometrics disproportionate to any intended benefit.

- *Least invasive alternatives should be considered:* A key part of a necessity and proportionality analysis is using methods with are least invasive to the privacy of an individual. Given the sensitivity of biometric data less, if a less invasive method for determining identity is possible then any digital identification program must adopt it while dispensing with biometrics. One such method is the use of one time passwords which offer multi-factor authentication beyond the input of the Aadhaar number. Even by the UIDAI's own authentication literature indicate that such a facility is available when it states that, "*[a] One Time Pin (OTP), with limited time validity, is sent to the mobile number and/ or e-mail address of the Aadhaar number holder registered with the Authority, or generated by other appropriate means. The Aadhaar number holder shall provide this OTP along with his Aadhaar number during authentication and the same shall be matched with the OTP generated by the Authority.*" [link] We further recommend that a facility of a smart card with technical controls to safeguard privacy and ensure security may also be explored.

- **Access and correction:**

  - *Biometrics are probabilistic:* Biometrics are inherently probabilistic (high chances of authentication failures of genuine persons), and they remain an experimental technology. This violates the principles of access and correction. As such biometric authentication captures distinct points of data and parses them through an algorithm that works on standards of probability. Such probability for matching biometrics violates the underlying purpose of data integrity even when access and a full recourse to correction [which is at present denied by Sections 28(5), 29 of the Aadhaar Act] is provided as greater accuracy which may come through such measures does not result in improved authentication. As explained by Paul De Hert in his chapter titled, "Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Distinctions" in Security and Privacy in Biometrics (2013), "*expectations in connection with biometrics are overestimated. Indeed, biometrics could lead to too much trust in the effectiveness of electronic solutions. Biometrics is based on probabilities: false positives and—negatives are unavoidable. If only one percent of a targeted group of 100,000 people a day suffers from a false negative, this would cause 1000 people every day to be incorrectly processed.*".

- *High error rates render access and correction nugatory:* Even reports which are largely uncritical of the Aadhaar project expressly note that, "*[w]hile Aadhaar authentication may reduce leakages, it can also result in beneficiaries—about one in seven in Andhra Pradesh and Telangana over FY 2016-17— facing transaction failures on Aadhaar-enabled ePoS devices.*" [Omidyar Network, State of Aadhaar Report 59 (2017) link]. This becomes more evident given the recent acknowledgment of the UIDAI that existing biometrics [thumb prints and retina scans] are unreliable for special categories of persons including senior citizens, where instead of dispensing biometrics itself it has now introduced the experimental technology of facial recognition [link]. Hence the rights of data subjects which are otherwise fulfilled by access and correction of their information are circumvented due to reliance on biometric technology.

- **Security:**

  - *Real time surveillance:* Biometric based authentication systems risk the security of persons as such biometrics are hardly secret being visible (iris) and open to capture (fingerprints). When utilised with public CCTV systems they lead to appreciable risk of real time surveillance of crowds down to a granular level of individuals. This increases the risk of profiling of individuals and further risks their security.

  - *Spoofing and vulnerability:* This point is succinctly captured by the LSE Study on the UK Biometric Program when it states, "*However, any claim of infallibility [on biometrics] is incorrect. All biometrics have successfully been spoofed or attacked by researchers. Substantial work has been undertaken to establish the technique of forging or counterfeiting fingerprints while researchers in Germany have established that iris recognition is vulnerable to simple forgery.*" [link] This same view is echoed by Juliet Lodge who in her chapter titled Nameless and Faceless: The Role of Biometrics in Realising Quantum (In)security and (Un)accountability in Security and Privacy in Biometrics (2015) notes that, "*The notion of the infallibility of a biometric is risky, over-simplistic and compromises individual and collective security primarily because a biometric is used as a tool for realising other purposes.*" Even the forthcoming introduction facial recognition technology has severe flaws and is an experimental stage which could be spoofed as little as by a person wearing sunglasses. [link] Hence, since the use of biometrics makes people more insecure rather than improve their security.

  - *Risk of data breach:* The Aadhaar Scheme due to it's design has been insecure and has been repeatedly breached revealing the demographic and aadhaar numbers of persons enrolled in this program [link and link]. A repeated claim

has been made by the UIDAI denying such leaks on the grounds that the biometric data stored in the Central Identities Data Repository are encrypted and cannot be leaked. This indicates that the biometrics which are collected of persons are stored in a central database, which increases multiple risks including data breaches through a single point of failure. There is no credible remedy if such biometrics are leaked and they will constitute a grave threat not only to individuals as there is no reset option for biometrics as there exists for non-bodily elements such as passphrases or digital ID cards. The likelihood of such a breach has been commented upon by expert cryptographer, Bruce Schneier who stated specifically in the context of Aadhaar that, "*When this database is hacked — and it will be — it will be because someone breaches the computer security that protects the computers actually using the data.. ...[t]ey will go around the encryption.*" [link]

Even beyond biometrics the universal reliance on the Aadhaar scheme by Central and State Governments, and especially the private sector, breaks data in silos (a unique identifier to be linked across databases enables pervasive profiling) and **violates purpose limitation**. The principle of purpose limitation has two ingredients namely, (a) a requirement that personal data processing must be for a specified, explicit and legitimate purpose; and (b) any further processing must be compatible with the original purpose of collection. The principle demands prior transparency of intentions (purpose specification) and binding to predetermined conditions (use limitation).

The Aadhaar system has been notorious for its mission creep and is being operated as a universal key to unlock passage to state and private services. A visible breach of purpose limitation is established in the following specifics:

- A unique identifier across databases: As stated above the Aadhaar database acts as a universal identifier for multiple databases and is not limited either to the purpose specification or sticking to the predetermined conditions. This is revealed by the indiscriminate use of biometric authentication and demographic data. Hence, even if it is presumed that there has been adequate notice and consent (which is absent as stated above), at the time such data was collected it is submitted that such notice being incredibly vague and indiscriminate has undermined the specification of purpose and the subsequent use limitation.

    - The pre-Aadhaar Act enrollment forms (significant as numerous enrollments done in the period of 2011-2016 prior to the statute) only listed limited consent at the time of enrollment when such demographic and biometric data was parted that, "*I have no objection to the UIDAI sharing information provided by me to the UIDAI with agencies engaged in delivery of public services including welfare services.*" [link] The generality is noticeable;

however it is evident even such a vague notice by itself does not permit the use of Aadhaar data for private service providers as being done at present.

- The post-Aadhaar Act enrollment forms (which may have gone through some iterations) contain a consent notice as, "*I am aware that my information including biometrics will be used for generation of Aadhaar and authentication. I understand that my identity information (except core biometric) may be provided to an agency only with my consent during authentication or as per the provisions of the Aadhaar Act. I have a right to access my identity information (except core biometrics) following the procedure laid down by UIDAI.*" [link] It is important to again consider that there is no purpose stated to the data collection except (a) enrollment to aadhaar; (b) authentication under consent or as authorized by the UIDAI. Hence, (b) again does not state the purpose which is again left vague to any use as may be determined by the UIDAI. There is a visible lack of any purpose specification or use limitation.

- Interlinked children databases: There are independent databases built off Aadhaar data which include the State Resident Data Hubs (SRDH) which provide a 360 degree view of individuals [link]. Such deep, pervasive surveillance that is built off both biometric and demographic data violates any meaningful understand of the purpose limitation [link].

We caution that any desire to provide legal sanctity to Aadhaar should not be merely restricted to the minimum threshold of a constitutional challenge but extend to its desirability and compliance with best principles. Hence, this committee is tasked with making recommendations which are not restricted to what is legally tolerable but also what is socially and constitutionally desirable. We urge for a complete review of the Aadhaar project particularly due it's conflict with personal privacy of individuals.

> "*...a thread running through all totalitarian systems from the prison to the authoritarian state is lack of respect for the individual's right to control information about the self. It has been said that mark of a civilisation can be seen how it treats its prisoners; it might also be seen in how it treats personal privacy.*"
>
> Gary Marx, Windows into the Soul 320 (2016). [Cited by Shyam Divan, Senior Advocate in their written submissions before the Hon'ble Supreme Court in *Justice KS Puttaswamy (Retd.) & Anr. v. Union of India & Ors* [W.P. (C) 494/2012]]

We submit that Aadhaar in its present form is incompatible with privacy principles and at the very least the following measures are required urgently:

(1) The recommendations of the committee should examine the Aadhaar project in its full ambit of practical execution, as well as it's purported legality -- as arising from the Aadhaar Act, 2016, to enable changes to its core features that are incompatible with a data protection statute.

(2) We support the use of digital technologies for public benefit, however, they should not be privileged over fundamental rights. Any digital identity scheme should be framed around the protection of individual rights through a data protection legislation, rather than a data protection legislation being framed to presumptively accommodate and work around an existing program such as Aadhaar.

(3) The following core features of the Aadhaar program are incompatible with the privacy principles:

(a) Compulsion in enrollment and authentication which negates principles of consent and choice. We suggest that the scheme should be made purely voluntary and existing Aadhaar users should be provided with an opt-out.;

(b) Reliance on biometrics as a method of enrollment and authentication which negates human dignity, necessity and proportionality and other principles. All biometric data should be deleted and a complete shift should be made to other forms of authentication such as OTPs;

(c) Universal reliance on the Aadhaar scheme by Central and State Governments, and especially the private sector, that breaks data in silos (a unique identifier to be linked across databases enables pervasive profiling) and violates purpose limitation. Separate schemes and digital identities should be implemented after viability studies that may be linked to digital keychains or management systems which work without pulling in meta-data and authentication logs across services.

(d) Absence of data breach notifications and credible remedies for individuals against the UIDAI which violates the principle of accountability. For this amendments are urgently necessary within the Aadhaar Act.

(4) The Privacy Commission should have overriding power and superintendence over the UIDAI. The UIDAI being a data controller and a data protection authority for Aadhaar data at the same time creates a conflict of interest.

Recommendation No. 5 : *An effective, citizen friendly adjudicatory system*

> *"Justice is in the outcome, and the procedure is a good one to the extent that it promotes this outcome.... Although the following analogy may strike some fans of procedural justice as a bit unfair, it seems to the outcome-oriented theorist as if a cook has a fancy, sophisticated pasta maker, and assures her guests that the pasta made in this machine will be by definition good since it is the best machine on the market. But surely, the outcome theorist says, the guests want to taste the pasta and see for themselves."*
>
> *Martha C. Nussbaum, Frontiers of Justice: Disability, Nationality, Species Membership 82 (2009)*

The success of any privacy law is dependent on the outcome and impact it can have through enforcement. An effective, citizen friendly adjudicatory system is an important step in delivering this promise. The recently released national economic survey 2017-18 points to endemic pendency, delays and backlogs which require foresight in the drafting exercise to prevent the orders of the privacy commission from turning into paper decrees. In addition to the tiered design of adjudication and investigation we endorse the suggestion on adequate funding specifically, "Government may consider incentivizing expenditure on court modernization and digitization. This needs to be supported with greater provision of resources for both tribunals and courts." [link].

We endorse the provisional view of the white paper which recommends an independent data protection authority, and suggest that this may be achieved through a tiered system of state level privacy commissioners and a central privacy commissioners. While individual complaints may be determined by the state privacy commissions, complaints effective to a class of persons should be made directly to the central privacy commission. Here, both the state privacy commissions and central privacy commissions should in addition to having the powers of a civil court also have the power to direct complaints to an office of a director general (similar to as one which exists under the Competition Act) which shall have investigatory powers.

We oppose any suggestion that complaints at the first instance may be made to the data controller or a privacy officer. Having such a formal limitation placed in law is likely to delay disputes and not result in any demonstrable benefit. We suggest, instead that, all original complaints may be made to state level and the central privacy commissioner. We suggest further that, the system of appeals may not be routed to any appellate tribunal given the long pendencies which exist. We further caution against the bifurcation of complaints between a special category dealing with monetary fines which may be routed through the system for adjudication of consumer disputes. Even this suggestion is likely to induce doubt, jurisdictional disputes (such as forum shopping) and is likely to result in uneven and inconsistent precedent even in instances where a cut-off such as a threshold is prescribed.

With respect to the penalties which may be the suggestion to prescribe upper limits in relation to a percentage of the worldwide turnover of a company is well taken and is in line with EU GDPR. We also support the payment of statutory damages to an effected class of persons through a data breach that may be determined by the Privacy Commissioner.

As the Justice A.P. Shah Committee noted that the existence of such specialised bodies should not prevent or hamper an access to justice. Hence, there should not be a bar to any claims before civil courts and the filing of criminal complaints with police. While the adjudicatory system put in place may be a proper forum, it should not be the sole adjudicatory system for an individual to seek redress.

To ensure an effective, citizen friendly adjudicatory system we suggest the following:

(1) Members of the public, in instances of disputes or allegations of violation of data protection regulations, should have the ability to make complaints to the Privacy Commission.

(a) Individual and class complaints should be made to the State Privacy Commissions.

(b) A class of affected persons (not necessarily a legal entity such as an association or registered body), or a representative action by an individual should be made directly to the Central Privacy Commission.

(c) The Privacy Commissions should have the ability to investigate (independently through the office of a director general), hold hearings and pass orders with directions and fines.

(d) Privacy Commissions should also file criminal complaints acting on such complaints.

(2) An appellate process to order for directions and fines should be to ensure deterrence and should require a pre-deposit of a percentage of the monetary fine prior to filing an appeal. Such statutory foresight is necessary to enable compliance and factor in a period of pendency at the stage of appeals.

(a) Statutory appeals from orders of the State Commissions should be appealable to the Privacy Commission.

(b) Orders of the Privacy commission should have finality and be statutorily appealable to the Supreme Court of India on restricted grounds of them

having a substantial question of law or an error apparent on the face of record.

(3) In addition to complaints to the Privacy Commission persons should have the remedy to approach the civil courts (even in instances where harm is suffered by a group of people) and file police complaints directly. We caution against the creation of any new adjudicatory tribunals or conferring exclusive jurisdiction on the existing ones as it is likely to create barriers to access to justice for the general public.

Recommendation No. 6 : A comprehensive data protection law is incomplete without surveillance reform

> *"Bentham's ideas for a prison form a philosophical base for a surveillance state with the State as a Panopticon all seeing and all knowing. Michael Foucault contended that the nature of the oneway surveillance in the Panopticon – what he referred to as the gaze – resulted in an asymmetry of knowledge, and hence power. Ultimately, Foucault argued, the omniscient surveillance created conditions whereby the observed themselves became instruments of their own suppression. So whereas Bentham viewed his Panopticon as a technology for reforming men, Foucault saw a method for creating docile bodies."*
>
> Meenakshi Arora, Senior Advocate in her written submissions before the Hon'ble Supreme Court in *Justice KS Puttaswamy (Retd.) & Anr. v. Union of India & Ors* [W.P. (C) 494/2012]

On the 14th of January 2018, it was revealed that the government of Uttar Pradesh had tapped more than 10,000 phones in order to catch two individuals who had dumped potatoes at various locations in Lucknow, as a form of protest [link]. This incident reveals the near-absence of an effective legal framework that regulates surveillance in India, and limits or prohibits bulk dragnet surveillance. The Indian Telegraph Act of 1885, and Sections 91 and 92 of the Code of Criminal Procedure, 1973 [link] provide a bare and unsatisfactory statutory framework for surveillance. Further, the specific rules framed under the Information Technology Act, 2000 for interception and surveillance allow for much more pervasive interception but remain deficient in protecting individuals. These laws are ill-suited for the 21st century, and insufficiently protective of individual rights. Further guidance is provided by a Standard Operative Procedure issued in 2014 [link], which contains a series of procedural checks, and specifies the (executive) authorities that are empowered to authorise surveillance requests.

Arbitrary, unreasoned and unregulated surveillance, especially when indiscriminately imposed upon a wide population, is a pertinent example of misuse of technology and a blatant violation of the right to Privacy. In this context, it is important to note that two

decades ago, a division bench of the Hon'ble Supreme Court in *PUCL vs. Union of India* (1997) 1 SCC 30 [link] made a crucial observation with regard to telephone tapping by the State:

> "*Telephone conversation is a part of modern man's life. It is considered so important that more and more people are carrying mobile telephone instruments in their pockets. Telephone conversation is an important facet of a man's private life. Right to privacy would certainly include telephone-conversation in the privacy of one's home or office.*"

The Court acknowledged the need for judicial scrutiny of the justifiability of surveillance as a precondition to such an action, yet ruled that it was for the Central Government to lay down the procedure by formulating Rules under the Indian Telegraph Act, 1885. What is most important to note is the *PUCL* judgment stressed the fact that surveillance, even when required, must be *targeted*, *necessary*, and *proportionate*. For example, Guideline 4 in *PUCL* stated that:

> "*The interception required under Section 5(2) of the [Telegraph] Act shall be the interception of such communications as are sent to or from one or more addresses, specified in the order, being an address or addresses likely to be used for the transmission of communications to or from, from one particular person specified or described in the order or one particular set of premises specified or described in the order.*"

Guideline 7 stated:

> "*The use of the intercepted material shall be limited to the minimum that is necessary in terms of Section 5(2) of the Act.*"

Reading Guidelines 4 and 7 together, it is evident that *PUCL* rules out the possibility of bulk or dragnet surveillance. The requirement that surveillance be targeted and minimal was endorsed by the Supreme Court in *State of Maharashtra vs Bharat Shantilal Shah*, while considering the MCOCA, and this reading of *PUCL* was endorsed by Justice Chandrachud in his plurality opinion in *Justice K.S. Puttaswamy vs Union of India*.

However, it must be noted that the safeguards laid down in *PUCL* were of an interim nature, a bare minimum, and a lower threshold of tolerable constitutionality --- and not sufficient to counter the various forms of illegal surveillance prevalent then, and more so in the present times. Indeed, with the advent in technology the platforms for data sharing have increased, private conversation has now moved beyond the telephone, into the CCTVs, the webcams, the social media, the Cloud. This has not only made the data more vulnerable to surveillance but has also made data protection more complex and necessary. In light of the *Puttaswamy* judgment, the right to privacy is a fundamental right which cannot be curtailed except according to "procedure prescribed by law", and that procedure must be necessary and proportionate. However, the surveillance programs conducted by the State have, so far, failed to adhere to the threshold set out in *PUCL*, and certainly fall foul of the standards laid out in *Puttaswamy*.

It is because of the ubiquity of surveillance and surveillance programs, that operate virtually unchecked (as the Uttar Pradesh potato dumpers surveillance example demonstrates), that a data protection law must squarely address the issue of privacy in the context of State surveillance. Over the course of the last few years, privacy violations have been more rampant in case of dragnet surveillance imposed on a large population (precisely what was prohibited by *PUCL*). For example, State sponsored projects like the CMS, NETRA and CID, are aimed at intercepting and collecting bulk data in the form of instant SMS, social media posts, VoIP calls, credit card details, bank transactions among others, on the stated ground of national security and anti-terrorism initiatives [link]. Not only do these programs violate the interim guidelines prescribed in *PUCL*, but they are also in violation of the Principles of Necessity and Proportionality [link] and the principle of Purpose Limitation as recognised by the Justice A.P. Shah Committee Report on Privacy [link], as also acknowledged by the Justice Kaul in the *Puttaswamy* case.

One of the major things to have plagued the country in this arena was undoubtedly the insufficient procedural safeguards adopted by the state in respect to the laws framed by the state. If the procedural safeguards are lacking in effectiveness, then the mere existence of the legislations does not help in curbing any menace as the primary objective behind the law which is the welfare and the protection of the interests of the state is inherently violated. Keeping in mind the grilling repercussions of the lack of procedural safeguards we analyse the operations which were undertaken by India under the *PUCL guidelines* and how on taking a closer look at the same one could discern that they were gung-ho at causing detriment to interests of the state at large working behind a good veil.

Another issue is the absence of any certain legality of the agencies which are permitted to conduct surveillance. NETRA was a tool developed by the Centre for Artificial Intelligence and Robotics (CAIR) of the Defence Research and Development Organisation ('DRDO') to analyse Internet traffic based on predefined filters.[link] It is unclear how the data to be analysed will be captured by the system, or whether this will be achieved through integration with the CMS. This lack of clarity is due the absence of any underlying law which would prescribe limits and safeguards.

While it is quite conspicuous that the Indian government is planning on launching many operations of mass surveillance, the distressing fact about this is that the details of the operation, the legal safeguards in place to protect the interests of the individuals, remain vague. As interpersonal communication is increasingly conducted digitally, it is inevitable that the state's intelligence activities are also increasingly focusing on the digital realm. What is worrying is the government's zeal in commencing these projects without specific statutory backing or oversight.

What was disturbing was that even before the CMS was deployed, the existing legal safeguards itself were not being properly followed. The government is alleged to have direct access to LIM equipment (which, in the case of an Internet Service Provider, is installed between its Internet edge router and its core network) through which the Government sends a software command and subsequently becomes eligible to suck out any information it wants without informing the subject. The lack of any sufficient safeguard allows the government to bypass existing legal safeguards including the requirement of an

interception order issued to the service provider by the competent authority.[link] Other legal safeguards – such as acknowledgment of receipt of an interception order by the service provider's nodal officers and the verification of interception orders every fifteen days between the service provider and the law enforcement agency – can easily be violated by law enforcement agencies without the service providers having any opportunity to identify the procedural defect.[link]

Another transgression is as follows: while the law requires interception orders to be tied to specific addresses, computer resources, or premises identified in the interception order, as mentioned in the IT act, in reality security agencies can conduct extremely broad searches using only keywords, which expand the scope of the search far beyond addresses, specific computer resources or premises helping them collect any information they want.

While the *Puttaswamy* judgment represents the culmination of the evolution of the right to privacy in India (beginning with Justice Subba Rao's dissenting opinion in *Kharak Singh v. State of UP* [link], a case that also concerned State surveillance, it would also be instructive to consider best practices from comparative jurisdictions, including jurisdictions where constitutional courts have had the opportunity to consider and adjudicate upon matters pertaining to surveillance, technology, and privacy.

The starting point for an examination of the right to privacy is Article 12 of the Universal Declaration of Human Rights (1948), Article 17 of the International Covenant on Civil and Political Rights, (1966) and the European Convention on Human Rights. In *Kruslin v. France* (1990), the European Court of Human Rights examined surveillance and held that "*it is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.*" Following this, in the case of *Kopp v. Switzerland* (1998), the European Court held that impugned surveillance measure should have some basis in domestic law; and it also referred to the quality of the law in question Notably, it held that tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence, and must accordingly be based on a 'law' that is particularly precise. This case clearly spelt out the need for a good law and parliamentary oversight over the operations of the surveillance, at whatever scale they were being conducted.

More recently, the debate surrounding mass surveillance became a burning issue, globally, after Edward Snowden's leaks about the American National Security Agency's glaring mass surveillance [link], encompassing citizens from other nations, including India. The debate has raised two pertinent questions :

- Firstly, to what extent is it justified to indiscriminately compromise on the privacy of individuals in the name of security strategies or terrorism prevention strategy?
- Secondly, are the current data protection laws are failing to protect the citizens' data from such international intervention?

As to the first question- the European Court of Human Rights, in the case of *Szabo` and Vissy v. Hungary* [link], has ruled against the legality of mass surveillance operations and stated that it:

> "*... condemns the vast and systemic blanket collection of the personal data of innocent people, often including intimate personal information; emphasises that the systems of indiscriminate mass surveillance by intelligence services constitute a serious interference with the fundamental rights of citizens; stresses that privacy is not a luxury right, but is the foundation stone of a free and democratic society; points out, furthermore, that mass surveillance has potentially severe effects on freedom of the press, thought and speech and on freedom of assembly and of association, as well as entailing a significant potential for abusive use of the information gathered against political adversaries; emphasises that these mass surveillance activities also entail illegal actions by intelligence services and raise questions regarding the extraterritoriality of national laws*".

For the purpose of clarity, mass surveillance is defined as a non-individualized non-transparent exercise which, in the absence of judicial scrutiny, has proven to an unreasoned and arbitrary encroachment upon the right to privacy. In view of the Indian Constitution, judicial precedents on the right to privacy, the *PUCL Guidelines*, the judgment in *Puttaswamy*, and international precedent, we suggest that bringing judicial expertise to bear in independently testing interception requests against the right to privacy may be the best method of protecting the right. Exercise of the judicial function could be guided by the "probable cause standard", which must be met by a law enforcement agency in order to receive an interception warrant.[link] The warrant procedure should be specified in the law. While the procedure need not be public, in order to preserve its confidentiality, but the Act should require that strict records of all warrant proceedings be retained, so that any illegalities can be subsequently detected and remedied.

The need for judicial scrutiny is highlighted by the April 2013 observation of the United Nations' Special Rapporteur on the Promotion and Protection of the Right to Freedom of opinion and Expression, who stated that the CMS was threatening to "take communications surveillance out of the realm of judicial authorisation and allow unregulated, secret surveillance, eliminating any transparency or accountability on the part of the State".[link] Furthermore, to cite an example of a legislation enacted by the UK after understanding the need for judicial scrutiny, we have the Investigatory Powers Act 2016, a comprehensive statute which made public a number of previously secret powers (equipment interference, bulk retention of metadata, intelligence agency use of bulk personal datasets), and provided for new safeguards wherein the warrants which were issued by the Secretary of the state required the approval of the judges before the operations came into force. [link][link]

As for the second question -- Justice A.P. Shah Committee, set up in 2012, has coined nine key principles of privacy which include- accountability, proportionality and necessity. The current State practices and laws regarding surveillance not only fail to adhere to these principles procedurally but also lack substantive alliance with them. The Committee had also made observations as to the irregularities and discrepancies between the two existing laws governing such interception and surveillance- the Indian Telegraph Act, 1885 and the Information Technology Act, 2000 [link].

Both of the acts contain different standards and procedures for interception through Rules. Broad similarities between the two include that authorization for interception must be based on executive orders, orders for interception must be reviewed by an overseeing committee, all interception orders must contain similar specified information, and every agency intercepting communications must establish similar procedures for the oversight, processing, conducting, and security of the interception. The Committee observed that the two laws differ vastly in several aspects including the grounds for interception/surveillance, the duration of data retention, the procedure, the standards to be followed, level of assistance from state agencies etc. This disparity is not only indicative of a non-uniformity in the regulatory regime which has led to inconsistency and non transparency, but it is also prone to misuse, and doesn't even lay out clear provisions as regards the redressal to the aggrieved individuals; it is also the reason for several loopholes in the safeguards governing surveillance projects. This regime nowhere states the necessity for judicial scrutiny or authorisation before the commencement of any of these operations which is exactly what should be done to forestall any arbitrariness on the part of the state. There are no sufficient safeguards to ensure that the interceptions do not invade privacy of any other individual other than the targeted one.

The existing laws complementing and supplementing this legal regime also need amendments. The most widely cited intention behind mass surveillance is national security and/or anti-terrorism initiatives. The data obtained through such surveillance is intended to be used as evidence against the suspects. Until and unless the admissibility of evidence obtained by infringing the right to privacy of individuals is questioned, establishing a fair surveillance regime is not possible. It is therefore crucial that such illegally obtained evidence is made inadmissible under the Indian Evidence Act.

Hence, to fulfill the objective of data protection, the need for consolidation of the laws governing surveillance- procedurally and substantively, is imperative.

We, therefore, recommend the following mechanisms to regulate and govern surveillance:

1. **State security agencies which intercept and record personal communications and data exist require statutory recognition. At the very least, they need to be brought within a system of parliamentary oversight.**

2. **Mass or, "dragnet" surveillance -- which is unrestricted surveillance directed over a group or class of persons should be prohibited in principle as contravening the principle of necessity, proportionality and purpose limitation.**

3. **Procedural safeguards for surveillance and interception orders needs to be strengthened as the existing are inoperational and deficient. We recommend several safeguards including prior judicial scrutiny in which public defenders are appointed on behalf of persons that will be surveillailed as well as notification of such orders to the subject of surveillance when it ceases.**

4. **We further recommend amendments to the Indian Evidence Act whereby evidence which is illegally gathered, such as telephone intercepts are recordings without valid tapping orders, are made inadmissible.**

Recommendation 7: *The right to public information needs to be strengthened and protected*

> *"The right to privacy and the right to information are both essential human rights in the modern information society. For the most part, these two rights complement each other in holding governments accountable to individuals."*
>
> > *David Amir Banisar, The right to information and privacy - balancing rights and managing conflicts, World Bank Institute Governance Working Paper Series* (2015).

The Supreme Court in the seminal case of *Secy. Ministry of Information and Broadcasting, Govt. of India and Ors. v. Cricket Association of Bengal and Ors.* (1995) 2 SCC 161 [link], held that, "[t]he right to freedom of speech and expression includes the right to receive and impart information. For ensuring the free speech right of the citizens of this country, it is necessary that the citizens have the benefit of plurality of views and a range of opinions on all public issues. A successful democracy posits an 'aware' citizenry. Diversity of opinions, views, ideas and ideologies is essential to enable the citizens to arrive at informed judgment on all issues touching them." Beyond treating citizens as mere passive recipients of information, the Right to Information Act has gone much further by being a watershed in citizen rights. It has brought greater transparency and accountability to public institutions furthering individual rights.

However, the right to information has sometimes been (incorrectly) posed as a competing or conflicting with the right to privacy. This conflict has been dealt within the Right to Information Act, 2005 which itself contains privacy protections. Section 8(1) of the RTI Act contains a list of various exemptions under which applications seeking information may be refused. Many of these rejections are based on privacy protection clauses. For instance, Section 8(1)(j) prohibits the disclosure of information which relates to personal information,or which would cause unwarranted invasion of an individuals privacy. Other provisions also provide a fairly robust privacy right,with Section 8(1)(d) taking care of trade secrets and the commercial interests of a third party and Section 8(1)(e) prohibiting disclosure of information held or gathered in the course of a fiduciary duty. However,all three clauses are subject to the rider that disclosure may be appropriate if it is determined that it serves a larger public interest. This is the consistent position taken by the act,which aims to promote transparency and accountability in the working of public authorities.

According to the 2010-2011 annual report of the Central Information Commission (CIC),this provision was the part of the act cited most frequently to turn down RTI applications; about one out of every four applications were rejected under it. Hence, there is no need for any amendments to the Right to Information Act, 2005 which by itself may even need further strengthening and support to further government accountability. As recently noted

by Anjali Bhardwaj and Amrita Johri, "Everything considered, given the extent of corruption and abuse of power in our country, there is clearly an overwhelming need to allow people access to information that would result in greater accountability." [link]

We are also concerned with a section devoted to the right to be forgotten. It is not clarified whether this would operate as a right to erasure of content or mere de-indexing of content on search engines. It is also not understood as to whether any such right will apply to public content or one which serves a public interest. Such a right may conflict with the fundamental right to freedom of speech and expression under the constitution of India requiring adequate safeguards (at the very least a judicial or an executive order as per Shreya Singhal v. Union of India) [link] and case-by-case adjudication. We would specifically refer to the case of *R. Rajagopal v. State of Tamil Nadu* 1994 SCC (6) 632 where the Hon'ble Supreme Court held that:

> *"A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child-bearing and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical... ...any publication concerning the aforesaid aspects becomes unobjectionable if such publication is based upon public records including court records. This is for the reason that once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment by press and media among others."*

We submit that the the right to public information needs to be strengthened and protected

(1) Individual rights are well served by the Right to Information Act which brings accountability to the functioning of government and public authorities. Hence, pre-existing privacy protections which exist under the Right to Information Act, and are contingent on public interest, need to be preserved and should not be subject to any legislative change by this committee.

(2) Specific and express language should be used exempting Information Commissioners from interference or control by the Privacy Commissioner and maintaining their independence.

(3) The, "right to be forgotten" or the right to de-indexing from search engines may undermine the fundamental right to free expression and should be developed within the framework of the privacy principles by the Privacy Commissioner rather than being expressly present in the statute. Given the journalistic and public interest in the maintenance of public information, sufficient safeguards need to be adopted.

Recommendation 8: *International harmonisation that recognises cross-border data flows to protect the open internet*

The interests of India and most stakeholders would be best served by a regime where we have a privacy and data protection law that is recognised as being of world standard,

harmonised with the models and legal structure of data protection regimes adopted by most progressive democratic nations. Such a regime has the advantage of ensuring that India can meet the adequacy requirements present in most such data protection frameworks, ensuring improved and smoother transfers of data from such nations to our own IT industry and software developers.

The rights of Indians with respect to their data is best safeguarded by a data protection legal framework which applies where-ever such data is transferred to in the world and one which would prevent such transfers in case adequate data protection standards or accountable legal process for such data transfers is lacking. The GDPR places an emphasis on a rule based framework to grant users control and accountability over their personal data. As was noted by the recent recommendations issued by the international non-profit organisation Access Now in its "Creating a Data Protection Framework: A Do's and Don't Guide for Lawmakers" [link]:

> "Recommendation 6 To Do: CREATE BINDING AND TRANSPARENT MECHANISMS FOR SECURE DATA TRANSFER TO THIRD COUNTRIES
> Data protection frameworks are designed to ensure the free flow of data by establishing adequate mechanisms for data transfer and effective safeguards for users' rights. These mechanisms must be put under strict and transparent oversight and include effective remedies to ensure that the rights of users travel with the data"

We believe that any legal framework for privacy and data protection must focus on this approach on ensuring secure data transfer via legal mechanisms for oversight and adequacy assessment, ensuring that Indians continue to possess - and be able to exercise - their fundamental rights with respect to their data no matter where it is transferred. Data localisation - when applied to the general, everyday web services and data that users engage with (rather than specialised sectors like sensitive government data) - would break our global open internet, and must not be considered.

(1) **Any data protection regulation must have extra-territorial effect and apply to web services and platforms which are accessible in India and which gather personal data of Indians. To ensure compliance, the Privacy Commission should also be empowered to confer adequacy status, in a transparent process, to foreign countries from which such global platforms carry out their operations.**

(2) **At the same time, care and caution should be taken to preserve the global character of the open internet which is beneficial to Indians as they can access information, knowledge and services from all over the world. Hence, any suggestions, such as blanket data localisation proposals, which would threaten and undermine the global open internet need to be resisted.**

(3) In the age of a global, open internet, our data protection framework must protect the data of our citizens globally and focus on interoperability.