To,
Justice Srikrishna and the Members of the Expert Committee on Data Protection,
Ministry of Electronics and IT,
Government of India.

Via:
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

Email: rakesh@meity.gov.in

Dated : Jan. 31, 2018

Subject: *Submission by Access Now to the Justice Srikrishna Committee of Experts on Data Protection*

Dear Sir,

We write to you in connection with the white paper ("**White Paper**") published by the Justice Srikrishna Committee of Experts on Data Protection, ("**Committee**") in November 2017 seeking public comments. This letter contains Access Now's initial comments in response to the White Paper.

Access Now is an international non-profit organisation which works to defend and extend the digital rights of users at risk globally. Through presence in 10 countries around the world, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. Access Now also engages with its global community of nearly half a million users from over 185 countries, in addition to operating a 24/7 digital security helpline that provides real-time, direct technical assistance to users around the world. We coordinate as part of CiviCERT (Computer Incident Response Center for Civil Society) a Trusted Introducer accredited CERT. We also have special consultative status at the United Nations.[1]

We recently filed on the TRAI Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector,[2] and have previously also provided inputs to the consultation organised by the TRAI on the topic of cloud computing. Members of our team have taken part

[1] Access Now, *About us*, https://www.accessnow.org/about-us/.
[2] Access Now, *Access Now comments to TRAI consultation paper on 'Privacy, Security, and Ownership of the Data in the Telecom Sector,* November 6, 2017 (Accessible at http://trai.gov.in/sites/default/files/AccessNow_07112017_0.pdf)

in the open house meetings organised by the Committee of Experts on Data Protection in Delhi and Mumbai across January.

We defend privacy and the rights of users to their data globally. Access Now provided comments on the development and implementation of data protection and privacy rules in the Brazilian Marco Civil,[3] the African Union Convention on Cyber Security and Personal Data Protection[4], and the broadband consumer privacy rules proposed by the US Federal Communications Commission, among other policy discussions in this sphere.[5] In the European Union, we have been involved in the EU Data Protection Reform process since the tabling of the General Data Protection Regulation ("**GDPR**") by the EU Commission in January 2012, and we have involved in the ongoing review of the EU e-Privacy Directive.[6]

Drawing from the lessons learnt from the extensive process for the formulation of the European Union GDPR, Access Now last week published a policy handbook titled "**Creating a Data Protection Framework: A Dos and Don'ts Guide for Lawmakers**" ("**Data Protection Guidelines**").[7] This paper was created to contribute to the global discourse on data protection and it particularly reflects on the approach the European Union has taken in the debate. In addition to our specific comments to the white paper, we attach the present paper ("**Annexure A**") to our formal submission.

Access Now has been actively involved at an organisation level with the annual International Conference of Data Protection and Privacy Commissioners (ICDPPC; https://icdppc.org/)[8]. Additionally, in relation to the right to be forgotten, we are attaching our global position paper for the perusal of the Committee - "**Access Now Position Paper: Understanding The "Right To Be Forgotten" Globally**" ("**Annexure B**").[9]

At the outset, we congratulate the Committee on the breadth and depth of the issues covered under the White Paper. As the world's second largest internet user base and with its history of

[3] Access Now, Brazil must protect the Marco Civil regulatory decree, June 2016. https://www.accessnow.org/brazil-must-protect-marco-civil-regulatory-decree/
[4] Access Now, African Union adopts framework on cyber security and data protection, August 2014. https://www.accessnow.org/african-union-adopts-framework-on-cyber-security-and-data-protection/
[5] Access Now, Comments on the FCC Notice of Proposed Rulemaking on protecting the privacy of customers of broadband and others telecommunications services, May 2017. https://www.accessnow.org/cms/assets/uploads/2016/05/NPRM-PrivacyofBroadbandCustomers-_-Access-Now.pdf
[6] European Commission, Responses to public consultation on the ePrivacy Directive, 2016. https://ec.europa.eu/digital-single-market/en/news/contributions-received-civil-society-and-consumer-associations-public-consultation-evaluation
[7] Access Now, Creating a Data Protection Framework: A Do's and Don'ts Guide for Lawmakers, January 2018, https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guilde-for-Lawmakers-Access-Now.pdf
[8] Accessible at https://www.accessnow.org/cms/assets/uploads/2017/08/NAVIGATINGHUMANRIGHTS_ICDPPC.pdf
[9] Accessible at https://www.accessnow.org/cms/assets/uploads/2017/09/RTBF_Sep_2016.pdf

seeking to advance strong, positive standards in favour of the rights of users as demonstrated by the February 2016 differential data pricing regulations issued by the TRAI and the 2017 ruling by the Supreme Court in the 9-judge *Puttaswamy* case, we believe India will play a crucial role in determining whether user privacy in their communications and data will be secured on our global internet. The Committee must act so as to help further this potential and the need to protect the rights of its millions of users online today, and the next billion soon joining.

Introduction

While the guidelines provides the essential elements to take note while devising a data protection regime, we submit that **privacy as a fundamental right** should be the guiding light of any such regime. The Supreme Court of India in its seminal judgement in the case of *Justice K.S. Puttaswamy vs Union of India*[10] has affirmed the fundamental right to privacy in India. The court not only affirmed the protection against the state an individual has, but also the positive obligation the state has in making the right to privacy a reality in India. As did the court in its judgement, the data protection regime to be created must also put the user at the centre of the law and **her rights must be viewed as as an end in themselves**. In this vein, we submit that the regime not be viewed as a "trade off" between business and innovation on one hand, and the user rights on the other.

The essence of our submissions flows from the Data Protection Guidelines, wherein we provide certain Do's and Don'ts in relation to formulation of any data protection regime:

Do's

1. **Ensure transparent, inclusive negotiations** - This includes conducting public consultations and expert roundtables, publishing negotiating texts and allowing comments from all interested parties with reasonable deadlines, and providing feedback on received comment. In all stages, meaningful participation from civil society groups must be ensured, and all meetings of decision makers with industry, NGOs, and consumer groups must be made public in an easily accessible registry. Maximum transparency around lobbying should accompany the process. Due weight should be given to input from civil society, to redress the inevitable imbalance in number of voices compared with industry

   In this context we note that certain reservations in relation to the inclusiveness, composition and the general procedure of the consultation and the committee have been raised by various organisations such as National Campaign for People's Right to

[10] (2017) 10 SCC 1

Information (NCPRI).[11] We support the NCPRI in such concerns and would re-iterate that for the drafting of a strong data protection framework in India, the ideals of transparency, fairness and inclusiveness must be incorporated into the process. As the old adage says - "*Not only must justice be done, it must seen to be done*".

2. **Define and include a list of binding data protection principles in the law** - Any framework aiming to protect personal information must include for instance a clear definition of personal and sensitive data. The level of protection should correspond with the sensitivity of each category of data.

3. **Define the legal basis authorising data to be processed** - Any entity, public or private, seeking to process personal data must abide by at least one of the legal bases provided for in the law. These usually include the execution of a contract, compliance with a legal obligation, and a user's explicit and informed consent.

4. **Include a list of binding users' rights in the law** - Users' rights, such as the right to object to processing of data, must be listed explicitly.

5. **Define a clear scope of application** - Lawmakers must clarify issues such as territorial or jurisdictional scope, given the need to ensure that users' rights are respected no matter where the entities using their data are located.

6. **Create binding and transparent mechanisms for secure data transfer to third countries -** These mechanisms must be put under strict and transparent oversight of a dedicated body and include effective remedies to ensure that the rights of users travel with their data.

7. **Protect data security and data integrity** - Engineers must consider data protection in the design phase of developing products and services, including setting the highest standards of protection by default. This concept of data protection by "design and default" should be spelled out in the law.

8. **Develop data breach prevention and notification mechanisms** - Lawmakers should create mechanisms for notification either within a data protection framework or in complementary legislation.

9. **Establish independent authority and robust mechanisms for enforcement** - Even the best data protection law in the world would be close to meaningless without an authority having the powers and resources to monitor implementation, conduct

[11] https://thewire.in/210668/activists-ask-committee-looking-into-data-protection-framework-to-be-more-transparent/

investigations, and sanction entities in case of (repeated, neglected, or willful) data protection violations.

10. **Continue protecting data protection and privacy** - No law is entirely "future proof". This means that a review process will likely be necessary — an opportunity to update the law, address any potential issues with compliance, and provide additional clarity and legal certainty where needed.

Don'ts

1. **Do not seek broad data protection and privacy limitations for national security** - Legislation should not give governments and public entities the capacity to shield themselves from the obligation to protect users' data. Governments not only have an obligation but also a security interest in ensuring the protection of personal data, especially when information is held by government agencies.

2. **Do not authorise processing of personal data based on the "legitimate interest" of companies without strict limitations** - Companies often argue that they should have a right to collect and process user data, without having to notify users. This contradicts the objective of data protection, which is to put users in control of their information.

3. **Do not develop a "right to be forgotten"** - The way several governments internationally have, accidentally or otherwise, misinterpreted the right to de-list or sought to extend its scope to limit freedom of expression or of information poses a significant threat to human rights.

4. **Do not authorise companies to gather sensitive data without consent** - The collection and processing of sensitive personal data should only be authorised when individuals have given their explicit, informed consent and have the right to withdraw that consent.

5. **Do not favor self-regulation and co-regulation mechanisms** - Self-regulation is not adequate as an enforcement mechanism and it is not sustainable for safeguarding individuals' rights.

Further, we submit our resonance with the data protection principles discussed in the report by the Committee of Experts on Privacy constituted by the Planning Commission under the Justice A.P Shah in 2012.[12] We submit that the following data protection principles should form the basis of the law in India:

[12] Accessible at http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

(1) *- **Fairness and lawfulness:** Personal data shall be processed fairly and lawfully which means that information should be processed on a clear legal basis, for a lawful purpose, and in a fair and transparent manner so that users are adequately informed about how their data will be collected, used, or stored, and by whom.*
(2) *- **Purpose limitation:** Personal data shall be collected and processed only for a specified and lawful purpose. This purpose shall be specific, explicit, and limited in time. Data shall not be further processed in any manner incompatible with that purpose.*
(3) *- **Data minimisation:** Personal data collected and used shall be limited to what is adequate, relevant, and not excessive in relation to a specific and defined purpose.*
(4) *- **Accuracy:** Personal data shall be accurate and, where necessary, kept up to date. Users shall have the right to erase, rectify, and correct their personal information.*
(5) *- **Retention limitation:** Personal data processed for any purpose shall not be kept for longer than is necessary.*
(6) *- **Users' rights:** Personal data shall be processed in accordance with the rights of users such as the right to access or right to erasure (See point 4).*
(7) *- **Integrity and confidentiality:** Personal data shall be processed in a manner that ensures state-of-the-art security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*
(8) *- **Adequacy:** Personal data shall not be transferred to a third country or territory, unless that country or territory ensures an adequate level of protection for the rights and freedoms of users in relation to the processing of personal data. Data protection frameworks shall provide for mechanism enabling the free flow of data between countries while safeguarding a high level of data protection.*

Following are the chapter-wise submissions:

1. Territorial Scope And Personal Scope

We submit that the territorial scope of any data protection law put the individual squarely at the centre of the legislation. The Committee must be congratulated on the provisional views published in this chapter.

We further note in our Data Protection Guidelines, under the specific principle of "***Define a clear scope of application***" - "*In the digital age, it can be difficult for legislators to ensure sufficient protection of personal data and the rights of users without applying the principle of extraterritoriality. To understand the benefits of the extension of the jurisdictional scope of data protection, we need to look at the issue not from an "establishment" perspective (where is the entity located?) but* ***from a user's perspective (where is the user and where is the user from?).*** *The objective of human rights law, such as data protection frameworks, is first and*

foremost to protect individuals at all times. It is therefore logical to ensure that users' rights are respected no matter where the entities using people's data are located."[13]

It is however also important to ensure that multiplicity of extra-territorial laws does not render itself to confusion or worse, propagation of rights-harming measures from states. It is essential that businesses be made aware of the applicable laws and the corresponding obligations such laws pose on them. We congratulate the Committee on noting the same in the point 5 of the provisional views in this chapter.

Further, **a one-size-fits-all solution or a blanket application of laws extraterritorially is not advisable**. The law must *"indicate under which scenarios the law applies outside their borders, to which actors specifically, what enforcement mechanisms will be in place, and provide users, companies, and authorities with clear avenues for remedies"*[14]*.*

More specifically, in relation to the provisional views under the White Paper, we submit that with respect to point no. 2 - "*However, it may be necessary to make the law applicable to all kinds of processing which the State may have a legitimate interest in regulating even though such processing may not be entirely based in India or may be carried out by non-Indian entities that do not have a presence in India*" - use of terms such as "*legitimate interest*" seems vague and the law must place the user at the centre of the law, rather than the interests of the state with respect to extraterritorial applications. In our guidelines, we note that in the digital age, it can be difficult for legislators to ensure sufficient protection of personal data and the rights of users without applying the principle of extraterritoriality, and therefore we strongly emphasise the following: "**To understand the benefits of the extension of the jurisdictional scope of data protection, we need to look at the issue not from an "establishment" perspective (i.e. "where is the entity located?") but from a user's perspective (i.e. "where is the user and where is the user from?")**. The objective of human rights law, such as data protection frameworks, is first and foremost to protect individuals at all times. It is therefore logical to ensure that users' rights are respected no matter where the entities using people's data are located."

We recognise however that extending the jurisdictional scope of a piece of legislation is not without risk and should be carefully considered by lawmakers. Conflicts of laws situations could arise and certain states could seek to extend the scope of rights-harming measures outside their borders using the same justification. Furthermore, not every entity processing data around the world knows about every country-specific law. It is often unclear whose obligation it is to inform businesses and individuals about their respective obligations and

[13] Data Protection Guidelines (Accessible at https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guilde-for-Lawmakers-Access-Now.pdf)
[14] Data Protection Guidelines (Accessible at https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guilde-for-Lawmakers-Access-Now.pdf)

rights. In our guidelines, we therefore recommend that awareness-raising campaigns be conducted to ensure that entities around the world know their obligations. In order for data protection laws to properly function, public authorities need the mandate and resources to carry out public education. Civil society can and should have an active role in the process, in particular to empower people to enforce their rights.

2. Other Issues of Scope

We congratulate the Committee on the provisional views provided under this section. We further note in the Data Protection Guidelines, under the specific principle of "***Define a clear scope of application***" - "*Finally, obligations under data protection law shall clearly apply to both the private and public sector. Public authorities are increasingly collecting individuals' information, getting access to private-sector databases, or otherwise building large databases of personal data. This processing shall be subject to clear obligations for the protection of individuals' personal information, the same way that processing by private entities is regulated.*"

With respect to point 2 of the provisional views in relation to this chapter, - "*The law may apply to data about natural persons processed both by public and private entities. However, limited exemptions may be considered for well defined categories of public or private sector entities*" - we submit that it is essential all public and private entities be subject to the data protection framework and the corresponding authority emanating from such framework. We submit that blanket exceptions not be made in application of the data protection framework with respect to any entity.

3. What is Personal Data?

We submit that personal data must be evaluated at the threshold of "**identifiability**". We broadly agree with the Committee's provisional views in this regard. However, we submit that the use of the term "reasonably identifiable" renders itself to unnecessary uncertainty. While we applaud the suggestion of providing code of conducts and guidance notes, we submit that the legislation err on the side of caution, and prescribe "identifiability" as the primary criteria. Data which becomes identifiable in the future due to technological advancements, should fall within the ambit of personal data at such time.

We welcome the suggestion of the Committee to include "*any kind of information including opinions or assessments irrespective of their accuracy*" within the ambit of data and personal data.

4. Sensitive Personal Data

We would like to submit that we broadly agree with the views of the Committee in this chapter. Further, we would submit that financial as well as biometric data should definitely be

considered as sensitive under the law. Additionally, the law shouldn't provide an exhaustive list of information which would be treated as sensitive. Rather, the privacy commissioner/authority should be allowed to develop on an inclusive list of data provided by the law, which would also serve as an indication of the kind of data which can be considered sensitive.

Lastly, we submit that higher standards of protection should be provided to sensitive personal data. For instance, such category of data shall only be processed on the basis of consent. We note the same in the Data Protection Guidelines - "***Do not authorise companies to gather sensitive data without consent***" - "*collection and processing of sensitive personal data shall only be authorised if individuals have given their explicit, informed consent and have the right to withdraw that consent subsequently*".

5. What is Processing?

We broadly agree with the provisional views of the Committee in this chapter. We applaud the view of incorporating both manual and automated processing along with online and offline processing within the ambit of processing.

6. Entities to be defined in the law: Data Controller and Processor

The analysis of the GDPR in the White Paper as regards to the definition and rules for controllers and processors is exhaustive. We appreciate the issues regarding the sharing of responsibility and liability between the various actors (such as controller and processors) involved in the data processing cycle.

In this context, the Article 29 Working Party - a body consisting of representatives from all data protection authorities of EU members along with the European Data Protection Supervisor and the European Commission - have provided guidelines which may prove useful in the settlement of this issue.[15]

7. Exemptions For Household Purposes, Journalistic And Literary Purposes And Research

In relation to exceptions made for "processing of data for research, historical or statistical purpose", we submit that while such exceptions are required, the law should clarify that this particular exception should be limited to when it is conducted "in the public interest".

In relation to the **proposed exception made for "national security"**, we recommend the following in our Data Protection Guidelines, under the specific principle of "***Do not seek broad***

[15] Accessible at http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf

data protection and privacy limitations for national security" - *"governments often seek limitations to data protection and privacy rights for their own use of personal data through the use of broad exceptions. These exceptions must be prevented and limited to clearly defined, necessary, and proportionate measures that include judicial oversight and accessible remedy mechanisms. Legislation should not give governments and public entities the capacity to shield themselves from the obligation to protect users' right to data protection.* ***Countries have a security interest in safeguarding personal data by government agencies."*** The Supreme Court of India in the *Puttaswamy judgement* notes the 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**. Similar observations have been by the report of the Committee of Experts on Privacy constituted by the Planning Commission under the Justice A.P Shah in 2012.[16]

In this regard, we would like to point the Committee's attention to the "***Necessary & Proportionate - International Principles On The Application Of Human Rights To Communications Surveillance***" - a set of interntional principles developed to guide communication surveillance with due regard to human right principles,[17] which were cited in the *Puttaswamy* judgment.

Further, in relation to the GDPR approach in this regard, while the Committee has noted Article 23 of the GDPR in its analysis, it would be important to note that **Article 23 of the GDPR on restrictions does also include a series of criteria that states must apply when such restrictions are being used** and that the restrictions does not apply to all obligations under the GDPR but some of them. Additionally, the EU has also developed a specific directive - **Directive 2016/680/EU** - which could provide further guidance on the use of personal data in the context of law enforcement.[18]

In its recommendations, the Committee must also emphasise that measures requiring the **mandatory retention of data** by private platforms via regulations or legal measures passed by the state are extremely harmful and impinge upon the right to privacy. In Europe, the Court of Justice of the European Union (CJEU) in December 2016 put an end to much of the debate surrounding the retention of telecommunications data in Europe. The CJEU gave a clear-cut interpretation of EU law regarding data retention, clarifying how it should be interpreted in national-level EU legislation. The ruling was in the joint cases of *Tele2 Sverige* (from Sweden) and *Davis and others* (from the UK), each of which stemmed from the 2014 *Digital Rights Ireland* (known as *DRI*) case.[19] That data retention mandates infringe fundamental rights and the rule of law was emphasised as recently as this week, with the UK Court of Appeals ruling in *SSHD v. Watson & Ors.* [2018] EWCA Civ 70 that the data retention mandate of the Data

[16] Accessible at http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf
[17] Accessible at https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf
[18] Accessible at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN
[19] Access Now, *Time's up! …for data retention mandates across the EU*, January 2017, https://www.accessnow.org/times-data-retention-mandates-across-eu/

Retention and Investigatory Powers Act (DRIPA), 2014 was unlawful. The law forced communications companies to store detailed information about the locations of people using devices such as mobile phones, as well as the who, when and how of every email, text, phone call and internet communication, and let public bodies grant themselves access to these personal details with no suspicion of serious crime and no independent sign-off.[20]

8. Cross- Border Flow of Data

In relation to cross border flow of data, we note that proper mechanisms for cross border flow of data are essential. We note in the Data Protection Guidelines, under the specific principle of "***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."*

Specifically, in relation to the GDPR, we note that the White Paper speaks of three mechanisms that can be used for transfer - adequacy, BCRs and MCCs under the GDPR. We note that these are not only the only mechanisms and transfer can also happen under certification, code of conduct and consent. The first two are new mechanisms under the GDPR. Further, Article 45 of the GDPR itself does not provide for an adequacy test as the White Paper indicates. The Article 45 language indicates that adequacy is a mechanism for transfer. However, the EU Commission has full discretion in granting adequacy and has a set of criteria for that purpose.

More broadly on the issue of cross-border jurisdictional issues, we have published specific policy information and guidance on the issues of the Mutual Legal Assistance Treaty (MLAT) system in the form of an online portal with information on such arrangements at MLAT.info[21] and a policy summary document[22] on proposals to further reform the global MLAT system which may be of use to the Committee.

9. Data Localisation

We would like to submit that the White Paper provides for ideas that data localisation is used to prevent foreign surveillance while also noting the the increased risk of local surveillance, in

[20] Liberty, *Court of Appeal rules Government surveillance regime IS unlawful,* January 2017, https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/court-appeal-rules-government-surveillance-regime-unlawful
[21] Accessible at https://www.mlat.info
[22] Accessible at https://www.accessnow.org/cms/assets/uploads/2017/07/MLAT-Reform-and-MLAT-Bypasses-one-pager.pdf

case of data localisation. However, we would submit that localised data is also not immune to access by foreign authorities.

We submit that we oppose mandatory data localisation measures which do not allow for transfer of data to third countries. Data should be protected at all time while stored and in transit. Mandatory data localisation undermines the fundamental openness and interoperability of the internet.

However, we also state that our position does not refer to data related regulatory measures for the protection of sensitive data existing in most of the states around the world which help governments for instance keep health, biometric or genetic data protected. In fact, such measures still allow for the transfer of data under specific circumstances that would ensure that the data remains protected during and after the transfer.

10. Allied Laws

We currently are not providing any inputs to this section.

11. Consent

We note in the Data Protection Guidelines, under the specific principle of "***Define legal basis authorising data to be processed"*** - *"Consent shall be defined as an active, informed, and explicit request from the user. It must be freely given and the user must have the capacity to withdraw consent at any time. This means, for instance, that pre-ticked boxes would not qualify as valid consent. In addition, companies cannot deny a user access to a service for refusing to share more data than strictly necessary for the functionality thereof. Otherwise, consent would not be freely given.*"

In this vein, we note "implied consent" contradicts the objective of putting user in control of their personal data as they might not be fully aware of the fact that their information will be processed. Consent must necessarily be an affirmative action.

As regards the discussion on consent fatigue in the White Paper, this paradigm is only applicable since often times consent is meaningless for users and not clearly explained. Consent shall be affirmative and informed in order for people to be empowered, in such scenarios consent fatigue will not be applicable.

Finally, we note the point made in the White Paper regarding the bargaining power of the contracting parties, and submit that the misuse of bargaining power can be prevented by incorporation of rules which preclude organisation from asking consent for data not required for the purposes of the services to be availed (data minimisation principle) as well as putting in safeguards which prevent organisations from denying services based on permissions not provided for "incidental data".

12. Child's Consent

We currently are not providing any inputs to this section.

13. Notice

To begin to meaningfully exercise their rights to privacy, a fundamental right that must be better protected in the digital age, **individuals require notice of where threats to their privacy lie.** Notice as a concept is married to consent. For adequate, informed consent, proper notice procedures are essential.

14. Other Grounds of Processing

On the point regarding legitimate interest, note our recommendations in our Data Protection Guidelines under the specific principle of "***Do not authorise processing of personal data based on the legitimate interest of companies without strict limitations***" - *"Organisations' legitimate interest is one of the legal bases that can be used to process personal data under the GDPR.*[23] *The core of data protection is users' control and predictability in the use of their data. The legitimate interest provision goes against these principles. Under "legitimate interest" an organisation is authorised to collect and use personal information without having to notify the concerned users. If you don't know that an entity holds data about you, how could you exercise your right to access the data or your right to object? We understand the need to provide companies with measures that allow them to conduct business, however, measures that prevent users from having control over their personal information shall be excluded as they contradict the spirit and objective of a data protection law. "* We shall also note that despite it flaws, the use of "legitimate interest" as a ground for processing under the GDPR still requires the data controller to consider the interests or fundamental rights and freedoms of the data subject to be valid.

Specifically, in relation to the provisional views under this chapter, we support point 4 regarding the lack of clarity of legitimate interest and few others ground for processing.

15. Purpose Specifications and Use Limitations

On the point regarding purpose limitation, note in the Data Protection Guidelines, under the specific principle of "***Define and include a list of binding data protection principles in the law"*** - ***"(2)*** - ***Purpose limitation:*** *Personal data shall be collected and processed only for a*

[23] See Article 6. 1. (f). European Union, Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

specified and lawful purpose. This purpose shall be specific, explicit, and limited in time. Data shall not be further processed in any manner incompatible with that purpose. ***(3)*** *-* ***Data minimisation:*** *Personal data collected and used shall be limited to what is adequate, relevant, and not excessive in relation to a specific and defined purpose."*

While we broadly agree with the analysis under this chapter, in relation to point 4 of the provisional views under this chapter - "*The use limitation principle may need to be modified on the basis of a contextual understanding of purposes and uses. This is captured by the reasonableness standard, i.e. a subsequent use is permitted as long as a reasonable individual could reasonably expect such use. This may be further developed by sectoral regulators."* - we submit that for any subsequent uses and purposes added by the data controller/processor, explicit consent and notice must be provided to the individual. It is only in such a circumstance, that the individual would have the ability to exercise their rights in relation to their data such as withdrawal of permission, access, and even questioning the legitimacy of the added purpose.

16. Processing of Sensitive Personal Data

We note that the references made to the GDPR in this chapter are accurate. We further note that the White Paper mentions "*It is also possible that personal or even non-personal data, when processed using big data analytics could be transformed into sensitive personal data. Therefore, there may be a need to create safeguards which will prevent misuse of personal information in these contexts of use.*" We support this objective, and the provisional views as well as the proposed law should incorporate such contextuals mechanisms while finalising the determination of sensitive personal data.

In addition, we submit that conversations on higher security standards for such data should be encouraged, and powers for best practice and standard setting - with adequate consultative mechanisms - powers be provided to the resulting Privacy Commission. Principles such as privacy by design must be adequately imported into the law for proper protection of data.

17. Storage Limitation and Data Quality

The White Paper in its provisional views in this chapter notes - "*Storage Limitation: The principle of storage limitation is reflected in most data protection laws and may consequently also find place in a data protection law for India. Further, it may not be feasible to prescribe precise time limits for storage of data since the purpose of processing will determine the same. However, the use of terms "reasonably necessary/necessary" may be employed and thereafter guidelines issued by the regulator, industry practices, interpretation by courts can bring clarity when it comes to implementation.*" While we agree with the broader principle elucidated here, we submit that reference to words such as "reasonably necessary" is vague. Given that data storage is directly linked to the purpose for which such data is collected, we suggest that reference should be made to "**necessary for a specified purpose**".

18. **Individual Participation Rights - I - Right to Confirmation, Right to Access, and Right to Rectification**
19. **Individual Participation Rights - II**

We note that this is a highly critical part of any data protection law. Under the Data Protection Guidelines, we provide the specific principle of "***Include a list of binding users' rights in the law"*** wherein the following principles are elucidated:

(1) ***Right to access*** *enables users to obtain confirmation from services and companies as to whether personal data concerning them have been collected and are being processed. If that is the case, users shall have access to the data, the purpose for the processing, by whom it was processed, and more.*
(2) ***Right to object*** *enables users to say "no" to the processing of their personal information, when they have not given their consent to the processing of their data nor signed a contract. This right to object applies to automated decision-making mechanisms, including profiling, as users have the right not to be subjected to the use of these techniques.*
(3) ***Right to erasure*** *allows users to request the deletion of all personal data related to them when they leave a service or application.*
(4) ***Right to rectification*** *allows users to request the modification of inaccurate information about them.*
(5) ***Right to information*** *ensures that users receive clear and understandable information from entities processing their personal data, whether these entities have collected this information directly or received it through third parties. All the information provided to the user shall be provided in concise, intelligible, and easily accessible form, using clear and plain language. This information shall include details about data being processed, the purpose of this processing, and the length of storage, if applicable. The entities shall provide their contact details and an email address to allow users to contact them in case there are issues.*
(6) ***Right to explanation*** *empowers users to obtain information about the logic involved in any automatic personal data processing and the consequences of such processing. This right is crucial to bring accountability and transparency in the use of algorithms to make decisions that impact users' lives.*
(7) ***Right to portability*** *enables users to move certain personal data they have provided from one platform to another offering similar services. To facilitate this process, interoperability between services shall be encouraged.*

Although this list is not exhaustive, these rights must be provided for by law, and not left to the discretion of entities using the data. Users shall be able to exercise any of these rights free of charge.

Specifically, in relation to **automated decisions**, we would note that while providing user with mathematical information regarding the functioning of an algorithm might not always be meaningful - it should nonetheless be available. It is important for entities using algorithm to take the burden of being explaining the information used, the processing of such information and whether new data (including insights and opinions) in relation to the user or otherwise, will be created.

Further in relation to point 2 of the provisional views in chapter 19, we while we applaud that we in India shall not import legitimate interest into the law, we submit that this fact should not preclude the existence of right to object to processing of data. We recommend consent to be defined as an affirmative action, rather than being implied. Additionally, it might be necessary for user to object to the processing of their information in certain contexts such as in relation to uses not envisaged in the original purpose.

20. Individual Participation Rights - III: Right To Be Forgotten

With respect to the Right to be forgotten, Access Now would like to present to the Committee our policy paper titled "**Access Now Position Paper: Understanding The "Right To Be Forgotten" Globally**".[24]

We would further note that the Right to be forgotten ("**RTBF**") should not require the deletion or erasure of content - RTBF as a concept more directly relates to creating a right to de-index information. The White Paper discuss erasure in the context of RTBF; this should be prevented. We submit that right to erasure and right to de-list are two separate rights. We further submit that we would recommend India not add such a right but in case the Committee is so inclined, it shall be limited to delisting and not lead to content being erased from online intermediary platforms. This approach balances the right to be forgotten with the right to free expression. We further submit that a right to erasure with respect to personal data when such individual leaves such a service should be provided.

Additionally, we note in the Data Protection Guidelines, under the specific principle of "***Do not develop a "right to be forgotten""*** - *"The "right to be forgotten" or "right to de-list" emerges from EU data protection law including the "Google Spain" ruling.[25] This right allows users under certain circumstances to request search engines to de-list web addresses from results when a search is done using their names.* ***This right should not be confused with the right to erasure which allows individuals to delete all personal data related to them when they leave a service or application.*** *The right to erasure is essential to ensure user control over*

[24] Accessible at https://www.accessnow.org/cms/assets/uploads/2017/09/RTBF_Sep_2016.pdf
[25] Court of Justice of the European Union, Judgement in Case C-C‑131/12, Google Spain SL vs Mario Costeja González, 13 May 2014. http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5eb572d024de249578524881c67efe5ec.e34KaxiLc3eQc40LaxqMbN4PaN0Te0?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=574499

personal information. It also should not be conflated with any take-down measure since the right to be forgotten developed under EU jurisprudence does not require or request any online content to be removed from the web or from search engine indexes. "

21. **Enforcement Model**
22. **Accountability and Enforcement Tools**
23. **Codes of Practice**
24. **Personal Data Breach Notifications**
25. **Categorisation of Data Controllers**
26. **Data Protection Authority**
27. **Adjudication Process**
28. **Remedies**

At the outset with respect to the enforcement models, we suggest the establishment of a Privacy Commission in India. In this regard, we would like to note from the Data Protection Guidelines, from the specific principle of "***Establish independent authority and robust mechanisms for enforcement***" -

"No data protection framework can be complete without a robust enforcement mechanism which includes the creation of an independent supervisory authority (data protection authority -- DPA -- or commission). Even the best data protection law in the world would be close to meaningless without an authority having the powers and resources to monitor implementation, conduct investigations, and sanction entities in case of (repeated, neglected, or willful) data protection violations.

Sanctions should be proportionate to the violations and can be in the form of notice to action. Authorities can for instance request a company stop certain practices that violate users' rights to data protection, such as the failure to provide a privacy policy or selling users' sensitive information without their knowledge and consent.

While punitive fines need to exist, data protection authorities shall apply limited fines to companies, in particular small SMEs, that do not engage in significant data processing, do not have the means to understand their obligations to respect data protection law, and have made mistakes out of ignorance rather than malice. Government shall also conduct awareness-raising efforts in order to avoid situations where companies would be ignorant of the existence and relevance of data protection laws. Tunisia, which is currently discussing its first ever data protection law, is proposing a quite innovative gradual approach to sanctions which includes higher fines in cases of recidivism.[26] As a result, a company found to commit data protection violations for which it has already been sanctioned would receive a significantly higher fine.

[26] Tunisia national authority for the protection of personal data. Article 211. Projet de loi relative à la protection des données personnelles, 2017. http://www.inpdp.nat.tn/Projet_PDP_2017.pdf

Sanctions and fines however represent only a small part of the work of DPAs. The role of data protection authorities is of course to enforce data protection laws and conduct oversight but also to assist organisations in their compliance duties. This means that companies, public authorities, and NGOs shall cooperate with data protection authorities to understand each other's duties and obligations. Organisations should not hesitate to establish contact with their DPA which can provide them with resources and materials to help implement the law.

Finally, DPAs have the powers to launch independent investigations into organisations and to hear cases brought to them by individuals or NGOs. In that sense, DPAs act as a guardian for users' rights and can help protect fundamental rights. These authorities are however still largely unknown by users around the world. To further help protect users' rights, NGOs should be empowered to represent users and to independently bring cases in front of DPAs and courts. Governments shall also further promote the work of DPAs, explain their role, and provide them with an adequate budget to ensure that DPAs can fulfil their duties."

In addition to the above, we further submit that the Privacy Commission have rule making powers, empowered on the basis of the data protection principles and the user rights as discussed above. Such rule-making powers should be subject to statutory requirements for adequate and meaningful public consultation and further mechanisms to allow for oversight by lawmakers over such delegated legislation.

Additionally, we would like to submit that the White Paper seems to indicate that the EU Directive on Data Protection from 1995 is a non-binding instrument and thus lead to interpretation. It may be noted that a directive is a binding legal instruments that set minimum requirement to all EU states to abide by. It does however leave room for interpretation and does not necessarily lead to full harmonisation as on a contrary a regulation would do. But the nature is definitely binding.

We further submit that self regulatory / co-regulatory models have not been successful in the world. In this regard, we would like to note from our Data Protection Guidelines, from the specific principle of "***Do not favor self-regulation and co-regulation mechanisms***" -

"*As more data are being shared online and offline, it is high time to develop mandatory frameworks for data protection and privacy all around the world to prevent or end these behaviours and put users back in control of their information. This will also enable the development of privacy-friendly innovation which is currently limited to a small number of companies that have undertaken a long-term engagement approach to protect their users instead of basing their business model in monetising users' private information. It cannot be relied upon, either from the perspective of individuals or businesses, due to the risk of "free-riding" by bad actors that will undermine privacy, trust, innovation and take-up of new products.*"

Additionally, we support and quote Prof. Graham Greenleaf's submission to this committee in this regard:[27]

"*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. 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.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 (i.e. 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. 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.*"

As regards fines and penalties, Page 28 of the White Paper discusses the fines under the GDPR referring to its application based on global turnover. In addition, the GDPR also set a figure for the fine as an alternative to the global turnover to ensure that fines are dissuasive. In fact, Article 83 says:

- *"be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding*
- *Financial year,* ***whichever is higher****"* (emphasis added).
- *"be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year,* ***whichever is higher"*** (emphasis added).

We support such fines, which are dissuasive, and submit that similar caps should be adopted under the Indian data protection law.

Lastly with respect to data breach notifications, we would like to note from the Data Protection Guidelines, from the specific principle of "***Develop data breach prevention and notification mechanisms***" - "*To prevent and mitigate these [data breach] risks, mechanisms for data breach notification and prevention of such breaches should therefore be developed, either within a data protection framework or in complementary legislation. High-profile incidents of*

[27] Accessible at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102810

personal data loss or theft across the globe have prompted wide debate on the level of security given to personal information shared, processed, stored, and transmitted electronically. In that context, gaining and maintaining the trust of users that their data are secure and protected represents a key challenge for organisations. The NGO Privacy Rights Clearinghouse have recorded 7,619 data breaches that have been made public since 2005 in the US alone.[28] *This means that at least 926,686,928 private records have been breached in the US since then. IBM and Ponemon Institute report that in 2017 the global average cost of a data breach is $3.62 million.*[29] *While this cost has slightly decreased compared to last year, the study shows that companies are having larger breaches. Other studies estimate that the average cost of a data breach will be over $150 million by 2020, with the global annual cost forecast to be $2.1 trillion.* [30] *This means that preventing and mitigating data breaches is not only good for users, but also good for businesses in order to save costs.*"

In conclusion:

We appreciate the Committee's openness in soliciting inputs in its consultations in this area. We believe that any future policy effort here must focus specific measures which help protect the rights of users, given the trust that such steps bring in the greater use of technologies.

We hope that we can be of assistance to the Committee as the development of a data protection framework advances in India.

Yours sincerely,

Raman Jit Singh Chima
Policy Director, Access Now

Naman M. Aggarwal
Asia Policy Associate, Access Now.

[28] Privacy Rights Clearinghouse, Data Breaches. https://www.privacyrights.org/data-breaches
[29] Ponemon Institute for IBM, 2017 Cost of Data Breach Study: Global Overview https://www.ibm.com/security/data-breach/
[30] The Experian, Data Breach Industry Forecast, 2015. https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf