Response Paper

For

Ministry of Electronics and Information Technology

on 'The Personal Data Protection Bill 2018'

October 2018

Background

Consumer Unity and Trust Society (CUTS)[1] expresses its gratitude to the Ministry of Electronics and Information Technology (MeitY), for inviting comments and suggestions on the Personal Data Protection Bill 2018 (The Bill).

About CUTS

In its 34 years of existence, CUTS has come a long way from being a grassroot consumer-centric organisation based in Jaipur, to opening overseas Resource Centres in Hanoi,[2] Nairobi,[3] Lusaka,[4] Accra,[5] Geneva[6] and most recently in Washington DC[7]. It continues to remain an independent, non-partisan and non-profit economic policy think tank, while opening various programme centres, namely: Centre for International Trade, Economics & Environment (CITEE);[8] Centre for Consumer Action, Research & Training (CART);[9] Centre for Human Development (CHD);[10] and Centre for Competition, Investment & Economic Regulation (CCIER).[11] It has been working towards enhancing the regulatory environment through evidence-backed policy and governance related interventions across various sectors and national boundaries. For further details regarding CUTS, please visit: http://cuts-international.org/pdf/About-CUTS-2018.pdf

Being a consumer-oriented organisation, CUTS has observed few critical issues in the Bill, which impede consumer welfare, either directly or indirectly as a result of sub-optimal regulation and competition in the market. These have been discussed in subsequent sections, along with a few recommendations to solve them.

[1] http://cuts-international.org/
[2] http://cuts-hrc.org/en/
[3] http://www.cuts-international.org/ARC/Nairobi/
[4] http://www.cuts-international.org/ARC/Lusaka/
[5] http://www.cuts-international.org/ARC/Accra/
[6] http://www.cuts-geneva.org/
[7] http://www.cuts-wdc.org/
[8] http://www.cuts-citee.org/
[9] http://www.cuts-international.org/CART/
[10] http://www.cuts-international.org/CHD/
[11] http://www.cuts-ccier.org/

CUTS' User Perception Survey

CUTS had commissioned a user perception survey pertaining to data privacy and user welfare in India. The objective of the survey was to gauge perception and experience of users with respect to privacy, purpose of data collection, usage of data collected, strategies for data protection, data breach, among others, in relation to data collected by online and offline service providers, as well as the government. A total of 2400 respondents (10 percent of whom were non-internet users) were interviewed across six states (one from each region – north, south, east, west, central and northeast) of the country. The sample was distributed between urban, peri-urban and rural areas, with adequate representation of respondents with different education levels, occupations, genders and age groups. In this context, few key findings from the survey have been incorporated in our submissions.

Key Submissions

The key recommendations of CUTS have been briefly laid out in this section. This is followed by the rationale/analysis validating our viewpoint.

Table 1: Key Recommendations of CUTS

SR. No.	Section	Issues/Findings	Recommendations
1	30(1)	More users were satisfied with the level of data security and online privacy at present when compared with their satisfaction level as of 2013. While 90% of users are aware of their privacy rights, only 47% of users exercise measures to enhance their privacy and protect data. The most common reason for non-usage of data protection tools was perception about their ineffectiveness in protecting data.	There is a high need for making data protection tools (such as cookie blockers, antivirus, etc.) effective. If such tools are best in class, service providers need to educate consumers about the effectiveness, utility and importance, and clear misconceptions about them, if any. This highlights the need and importance for undertaking capacity building workshops for consumers to enhance the uptake of data protection tools, with support from well-established and credible consumer organisations. The Bill should mandate such responsibilities on data fiduciaries, taking into account their level of interaction with consumer data, and relevant provisions may be incorporated in the said section.
2	39	Majority (60%) of the users were satisfied with online service providers from a privacy perspective, while only 2% users perceived to have experienced violation of privacy and data breach. Notably, 53%	The survey highlights the need to improve privacy regime through capacity building and awareness programmes, with special focus on identifying privacy violation, data breach and grievance redress measures. It also brings forth the need to make the process of grievance

SR. No.	Section	Issues/Findings	Recommendations
		of such users went on to report the violation to seek redressal.	redressal more consumer- friendly by adopting simple procedural mechanism. The Bill should have a clear time frame for resolving complaints. The regulator could provide regular updates to complainants on the progress of their complaint through a communication channel of their preference.
3	3(29)	Consumers' deem email IDs to be more sensitive when compared with other details like name, age, gender, contact number and address. This might be because consumers are of the opinion that it might be easy to identify them from their email IDs, when compared with other details mentioned above.	The test for establishing 'identifiability' should include consumer perspective. The select range of personal identifiers should be informed by the perception of consumers, and mentioned in the Bill.
4		Users are not comfortable in sharing their personal views (on religion and politics), financial details and medical history, as they may regard them to be 'extremely personal' or 'intimate'.	The use of sole criteria of 'identifiability' for defining personal data needs to be revisited. Adequate consideration should be given to other criterion as well such as users' comfort (irrespective of its relevance in identifiability) in sharing different types of data.
5		Most users believe they are not sharing their personal photos, videos and exact location, with any service provider or government despite reliable reports having contrary viewpoint.	In order to make provisions of the Bill effective, there is a well-established need to generate awareness and build capacity among consumers on concepts of personal data and sensitive personal data.
6	26(2)	The value of non-automated and /or offline data is no less than data shared online.	The right to data portability (inclusive of data retrieval and data transfer) should also be extended to non-automated data processing and data collected through offline means. Capacity building, awareness generation and advocacy can help in bridging the existing constraints of implementation of such a provision.

SR. No.	Section	Issues/Findings	Recommendations
7	8(1)	Businesses should not be allowed to use consent notices and privacy policies as a means to shrug away their liability. Rather the essence behind privacy and data collection disclosure must be to educate the consumer about the business' data use practices. The user perception survey highlighted that at present, a very limited number of users were reading privacy policies. Among those who were reading, most of them did not understand them.	The notices and policies should be simple, easy to understand and technology should be used to address any doubts that users may have. The users should also be in a position to compare consent notices, privacy policies and practices of different data fiduciaries on indicators like length, availability in different languages, and use of legal language. Relevant information should be publicly available on the web site of the proposed Data Protection Authority (DPA). Also, data auditors might assess the user friendliness of privacy policies, while undertaking audits and providing data trust scores to data fiduciaries.
8	40	The observation of the Committee must be treated as a recommendation, i.e. *India would have to carefully balance possible enforcement benefits of localisation, with the costs involved in mandating such a policy in law*.	It is recommended that the regulation making process be more balanced and pro-active, instead of being merely a reactive one. Regulations can have varied and divergent impacts on different stakeholders, and it is thus necessary to ensure that in the process of achieving its objectives, the costs imposed by regulation on stakeholders do not outweigh its benefits. Moreover, assumptions and fear ought to be replaced with evidence-based research from various perspectives – economical, social as well as civil liberties. Accordingly, undertaking Regulatory Impact Assessment (RIA) or Cost-Benefit Analysis (CBA) of the proposed data mirroring and localisation mandate becomes imperative in order to map their impact on various stakeholders before enactment.
9	35(2) & 35(6)	Users understand the benefits that digital technology provides. Reputation of a service provider is a key parameter to decide whether users would like to share their data or not,	The trust scores should factor in reputation of the service provider; easy to read privacy policies; anonymisation of data; having appropriate consent and notice mechanisms; flexibility in providing data (providing limited data

SR. No.	Section	Issues/Findings	Recommendations
		reflecting the importance of trust between users and service providers. Users have high expectations of privacy from service providers which service providers must live up to for maintaining trust. While assigning a rating in the form of a data trust score to various service providers/ data fiduciaries, it might be pertinent to examine the issues users consider important while deciding to share data.	for availing limited service); number of mobile app ratings and number of downloads; knowledge of the data fiduciary's data protection measures; and tools offered by the data fiduciary to the data principal for data protection. Alternatively, Trustmarks or Trustseals could be used as a certification of trustworthiness which demonstrates accountability. Such marks/ seals assign recognition on the basis of set standards and practices, and therefore, minimise subjectivity and maximises credibility. However, such standards could be jointly developed by the regulator and other stakeholders.
10	68(2)	The adjudicating wing within the proposed Data Protection Authority is intended to be quasi-judicial body, while the Central government, which is a part of the executive, will prescribe the operation, segregation, independence and neutrality of the wing. There might be instances where the government is a party to a dispute. In such a case, there would be a conflict of interest as the government would be a party to the dispute before the adjudicating wing, and will also have the power to appoint members to the adjudicating wing.	Thus, there is a need to amend 68(2) of the Bill to make the adjudicating wing truly independent and ensure transparency and accountability. CUTS' suggestions on the Regulatory Reform Bill may be taken into account in this regard.[12]

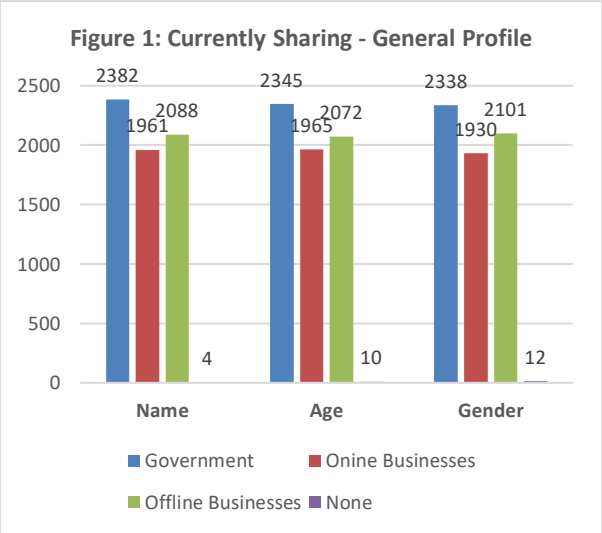
[12] http://www.cuts-ccier.org/event-Regulatory_Reforms_in_India-A_Roundtable.htm

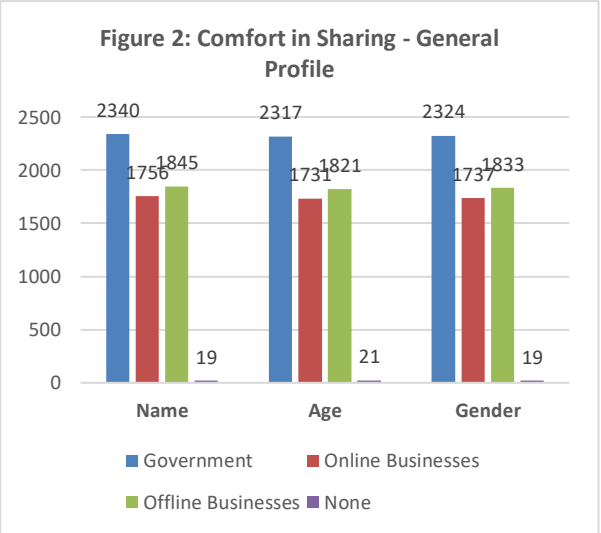
Detailed Submission

Definition and Scope of 'Personal Data'

While Section 3(29) of the Bill defines 'personal data', the definition may be subject to varying interpretation resulting in vagueness. It might be useful to provide some examples to elaborate on concepts mentioned in the definition, such as 'identifiability'. In this regard, it will also be important to consider consumer perception with respect to different kinds of data.

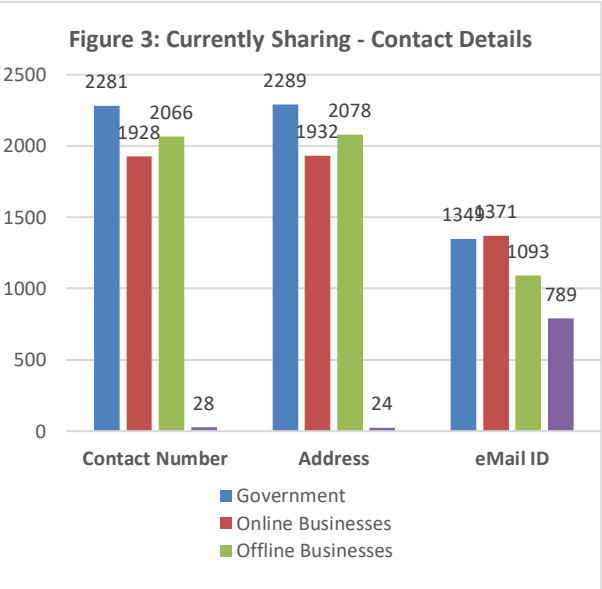
Based on the User Perception Survey conducted by CUTS, it appears that most consumers think that they were currently sharing their name, age and gender with online and offline service providers and the government. Most consumers were comfortable in doing the same.

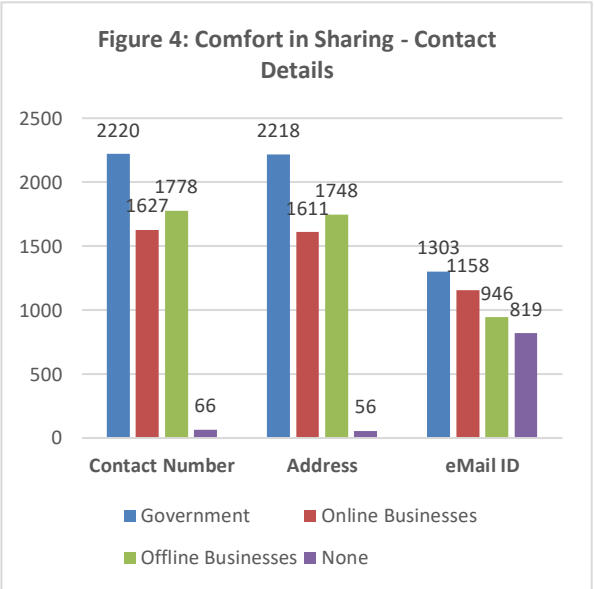




Slightly lesser number of consumers thought that they were sharing contact number and address with such service providers. A corresponding comfort level was witnessed with respect to sharing such details. However, a significantly lesser number of consumers thought that they were sharing email IDs with service providers. Corresponding lower comfort level was visible with respect to sharing of email IDs.

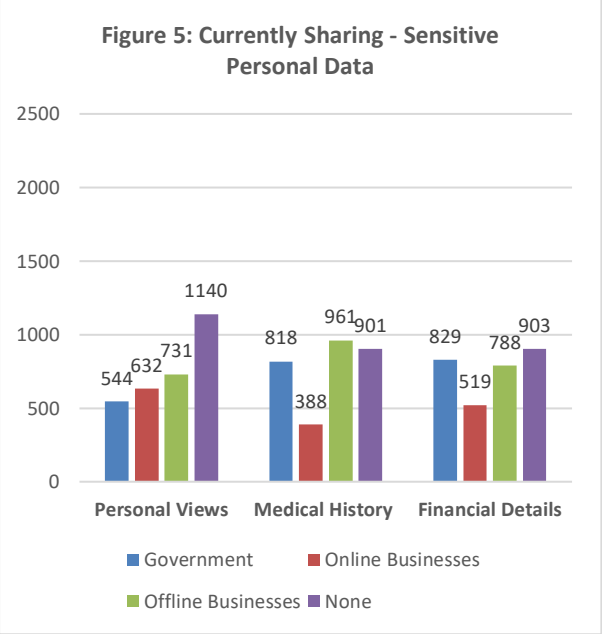
Consequently, it appears that consumers deem email IDs to be more sensitive when compared with other details like name, age, gender, contact number and address. This might be because consumers think it might be easy to identify them from their email IDs, when compared with other details mentioned above. Consequently, the test for establishing 'identifiability' should include consumer perspective.

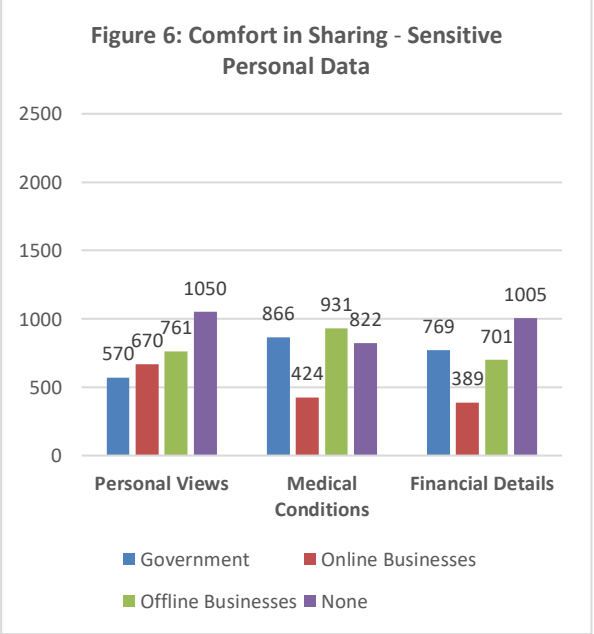




The survey also highlighted that users were not sharing, and neither were comfortable in sharing their personal views (on religion and politics), medical history and financial details with online and offline service providers or with government.

While this might be on account of users' concerns with respect to 'identifiability', but the same might not be the sole reason. Users might not be comfortable in sharing these details, as they can consider them to be 'extremely personal' or 'intimate'.

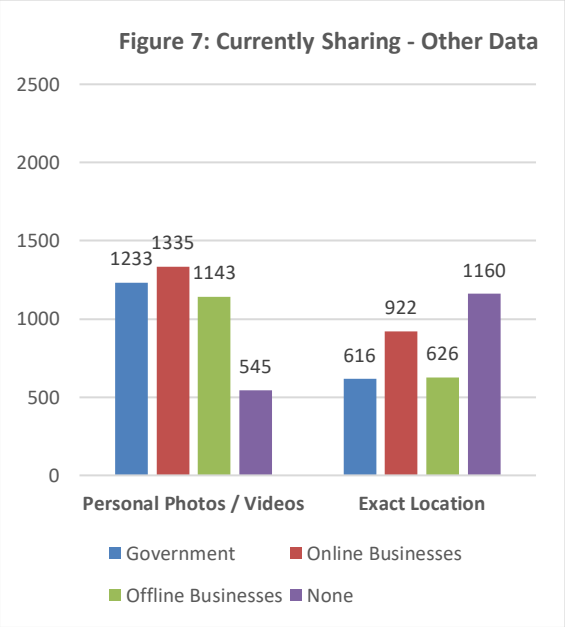


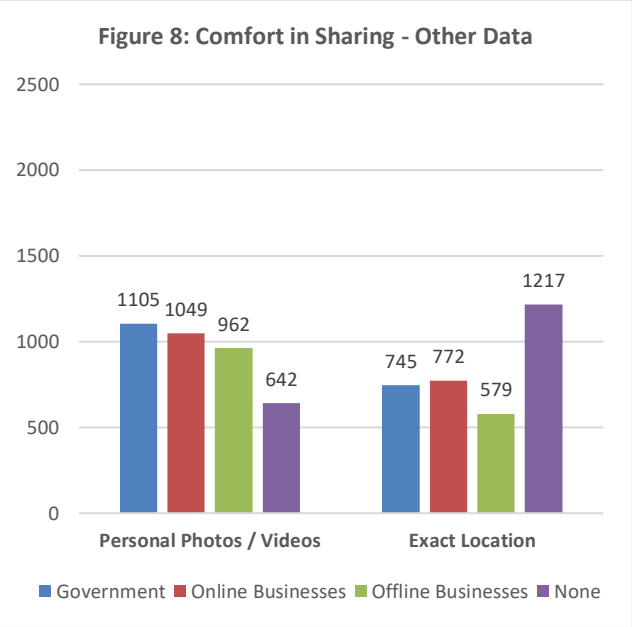


Consequently, the use of sole criteria of 'identifiability' for defining personal data needs to be revisited.

Interestingly, it appears that users also treat data like personal photos, videos and exact location with extreme sensitivity. **Most users believe they are not sharing such data, particularly location, with any service provider or government despite reliable reports to the contrary. Consequently, in order to make provisions of the Bill effective,**

there is a well-established need to generate awareness and build capacity among users on concepts of personal data and sensitive personal data. Such activities should be supported by data fiduciaries, and implemented by well recognised consumer groups.





There might also be merit in defining the scope of 'personal data' and 'sensitive personal data' based on perceived risk of misuse by the user, which is not necessarily similar to the 'identifiability criteria'.

Scope of Data Portability

The Bill restricts the right to data portability under Section 26(2) to data processed through automated means. As revealed in CUTS user perception survey, in many instances, data is collected through non-automated means and offline means, such as by doctors through prescriptions, etc. The number of users sharing data through non-automated and offline means is often higher than the number of users sharing same data through online means.

Consequently, the right to data portability (comprising right of retrieval and transfer to other data fiduciaries) should also be extended to such non-automated data processing. Furthermore, the scope of the said provision may also be extended to data collected through offline means. While there may be questions with respect to implementability of such provisions, the value of offline data is no less than data shared online. Capacity building, awareness generation and advocacy can help in bridging the existing constraints.

The CUTS' survey mapped user perceptions with respect to data collected by online businesses, offline businesses and the government, on various aspects, such as expectations, comfort levels, satisfaction levels, etc. Any rights being given to data principals must be extended to data collected by all these three service providers. Accordingly, the right to data portability must be extended to offline data and data processed through non-automated means.

Consent and Notice Mechanism

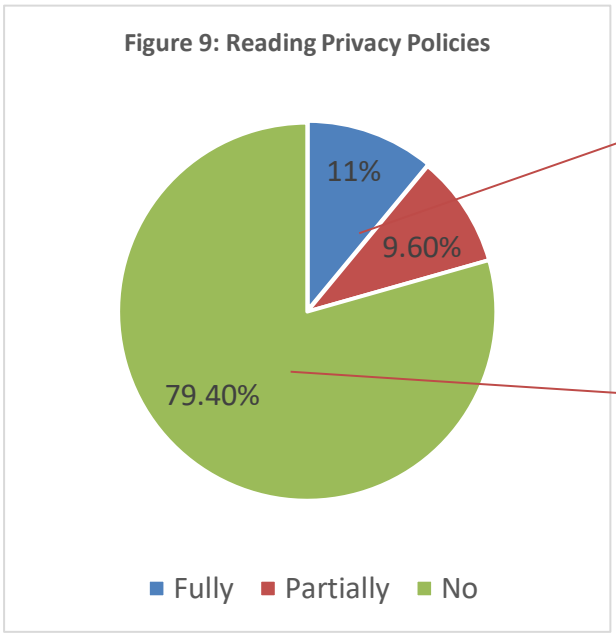
The Bill has laid down important requirements for a valid consent – free, specific, informed, clear and capable of being withdrawn. These are in line with Article 4(11) of the European Union's (EU) General Data Protection Regulation (GDPR). However, elaboration on each of these requirements and indication on manner of compliance is missing. For instance, Article 7(2) of the GDPR requires the data controller to present the request for consent in an intelligible and easily accessible form, in simple and clear language.

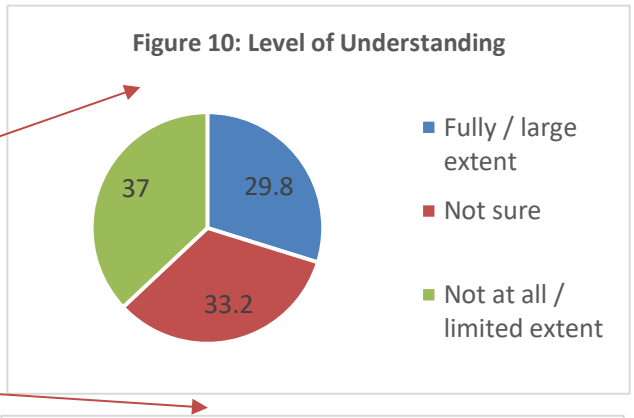
Apart from the provisions of GDPR, one must also refer the Indian Contract Act, 1872 to gauge the essentials of a valid consent. Section 13 requires the parties to a contract to agree upon the same thing in the same sense. However, it needs to be realised that this might be difficult given varied socio-economic, education, occupation and demographic factors in a diverse country like India.

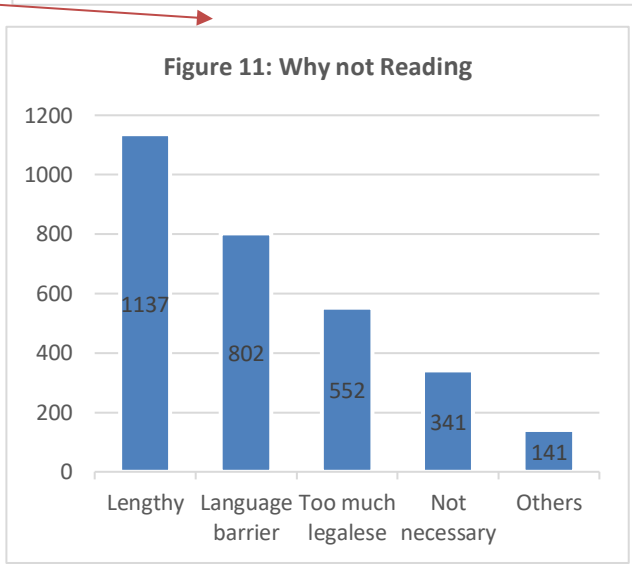
Consent should signify informed choice, which might not be the case for consumers at present while accepting notices and privacy policies. This is evident through the lengthy and incomprehensible language of such notices and policies, full of legal jargon. Going forward, businesses should not be allowed to use consent notices and privacy policies as a means to shrug away their liability.

Rather the essence behind privacy policies and data collection disclosure must be to educate the consumer about the business' data use practices. In order to comply with the requirements under the Bill, in case practices that exist today continue, the objective of specifying principles of consent, as mentioned above, might be lost.

The user perception survey highlighted that at present, a very limited number of respondents were reading privacy policies. Among those who were reading, most of them did not understand the same.

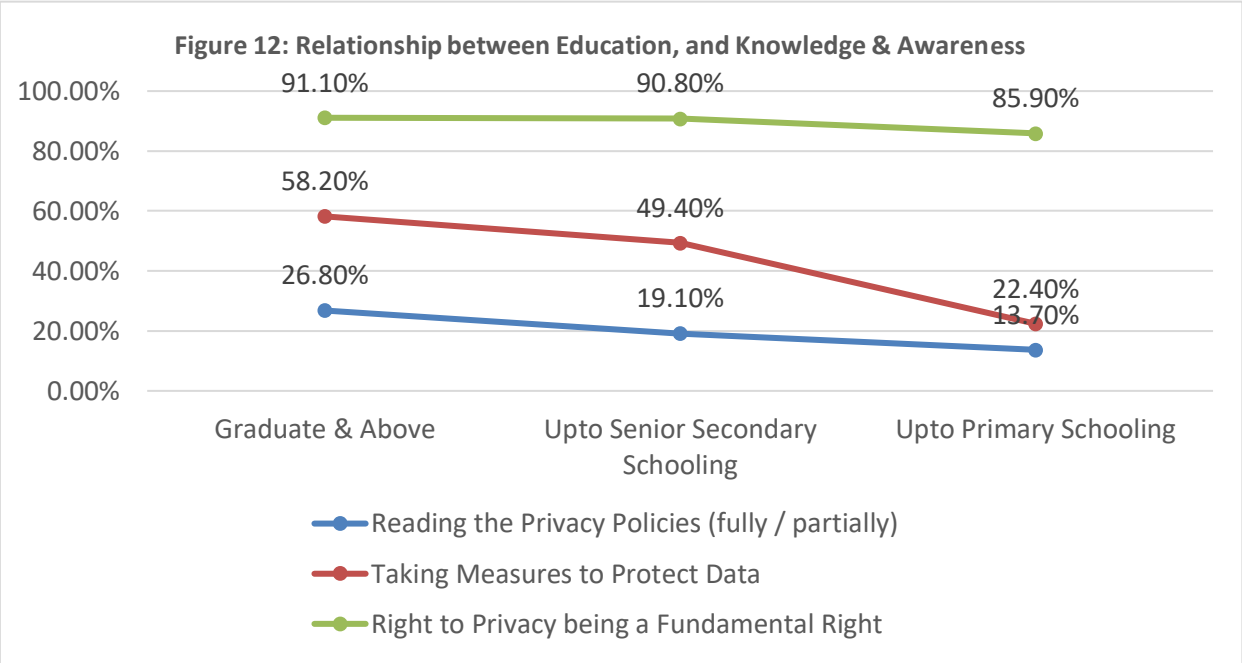






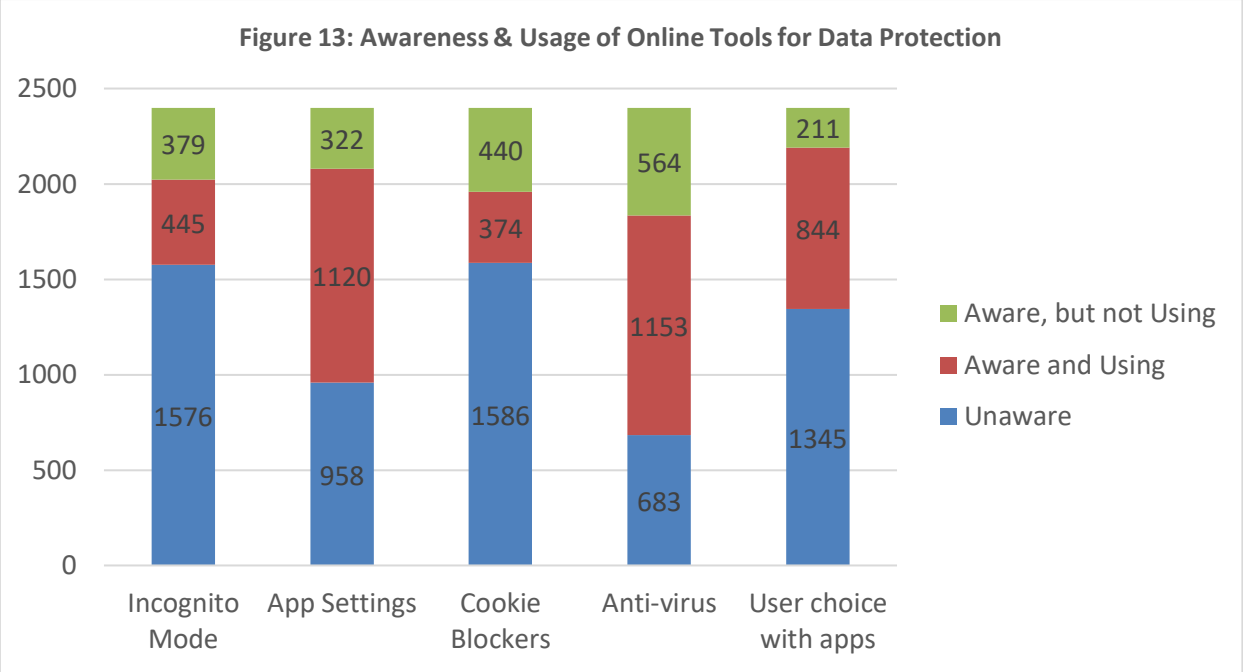
The reasons for not reading the privacy policies relate to length, language and terminology, among others. Consequently, the Bill should provide principles to address such concerns in privacy policies. The policies should be simple, easy to understand and technology should be used to address any doubts that users may have. The users should also be in a position to compare privacy policies and practices of different data fiduciaries on indicators like length, availability in different languages, and use of legal language. Relevant information should be publicly available on the web site of the proposed Data Protection Authority. Also, data auditors might assess the user friendliness of privacy policies, while undertaking audits and providing data trust scores to data fiduciaries.

While enabling active and informed consent is necessary, it is also be important to ensure that consumers are able to adequately comprehend the implications of their consent, on their data/informational privacy. CUTS' user perception survey pointed out that users are mostly aware that 'right to privacy' is a fundamental right. However, users were not

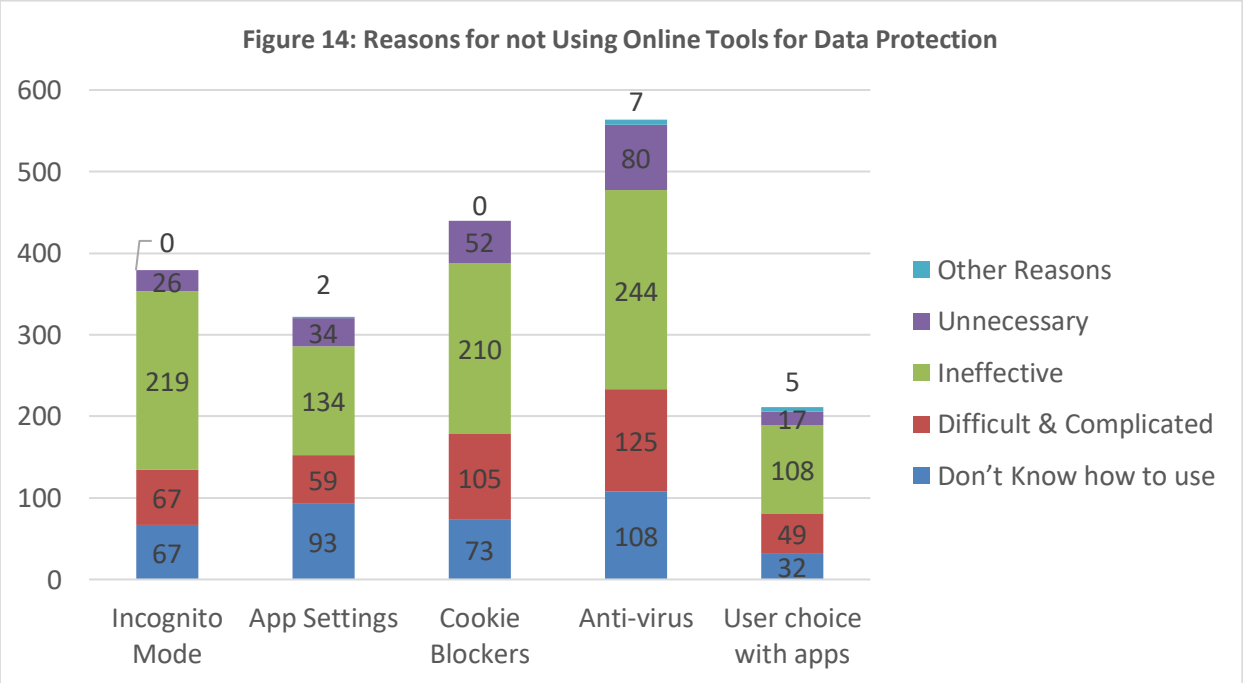


exercising this right (or were not in a position to exercise this right) since they were neither reading (or were unable to read) the privacy policies of various service providers (government, online and offline businesses), nor were they taking (or were unable to take) extensive measures to protect their data. Furthermore, it was observed that the lower the education level of consumers, the lower was the possibility of taking measures.

It was further observed that many users were not aware of popular tools for data protection, such as incognito mode, cookie blocker, or exercising choice with mobile apps. Most popular tools were anti-virus and app settings. The latter is very important as majority of Indians access internet over their mobile devices and through apps. There is a need to raise further awareness about the various measures that the consumers can use for protecting their data.



The most common reason for non-usage of data protection tools was perception about their **ineffectiveness** in protecting data. Consequently, there is high need for making such tools effective. If such tools are best in class, service providers need to educate public about their effectiveness, utility and importance, and clear misconceptions about them. The Bill should mandate such responsibilities on data fiduciaries, taking into account their level of interaction with consumer data.



Other reasons for not using data protection tools include them being difficult and complicated and users not knowing how to use such tools. This strengthens the case for capacity building of users.

In addition to addressing the issue of privacy policies and user capacity, the concerns with respect to consent and notice fatigue also need to be addressed. It has been pointed out that

at present, reading the privacy policies of all the regularly visited web sites by consumers in a year, has been estimated to take about 244 hours. Therefore, the large opportunity cost associated with such an effort, may not make it reasonable to expect consumers to provide meaningful consent to sharing their data, after reading such privacy policies.[13]

Further, it has been observed, that privacy policies are displayed at inconvenient times, thereby conflicting with the consumers on-going actions, thereby being accepted without any thought. Added to this, even businesses are to lose on account of consent fatigue, since they run the risk of losing new consumers, who do not take the time to accept an exhaustive privacy policy.

It becomes important to understand the implications of Section 8(1) of the Bill with respect to the issue of lengthy consent and notice requirement. The exhaustive list of information to be furnished to data principals, if presented in its current form may lead to consent and notice fatigue. It might further result in data fiduciaries having lengthy and technical privacy policies, which might prove to be counter-productive to obtain valid consent from their consumers.

CUTS' recommends the inclusion of an 'Executive Summary' in privacy policies. In other words, the most important information required at the time of notice for consumers must be formulated in a more participative manner, by taking the views of consumers through primary interaction with them, and creating a feedback loop, in order to gauge their understanding of policy. **An approach adopted in the financial sector wherein Most Important Terms and Conditions are highlighted upfront in bold and bigger font size may be adopted.** A human-centred design approach can be formulated in this regard.

Transfer of Personal Data outside India

Most debates on the issue of transfer of personal data outside India, data mirroring and data localisation have happened from the perspective of businesses and government. Consumer perspective on this issue, despite being important, has been mostly ignored.

CUTS International recently organised a roundtable on '**Consumer Sovereignty in the times of Data Localisation**' to discuss consumer perspective on these issues. ***The report is accessible here.***[14]

A summary of findings and recommendations on this issue, based on primary and secondary research are given below:

Impact on Consumers

- Free services available to consumers may become chargeable due to the enhanced cost of compliance on businesses, which will ultimately trickle down to consumers. Alternatively, the cost of existing paid services may also go up on account of such measures.
- Certain businesses may exit the Indian market (or foreign business, especially foreign small and medium enterprises, may not be in a position to enter Indian market), leading to unavailability of their services for Indian consumers. This may result in reduced

[13] http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Cranor_Formatted_Final.pdf
[14] http://www.cuts-ccier.org/Event-Round_Table_Discussion_on_Consumer_Sovereignty_in_Times_of_Data_Localisation-Sep6-2018.htm

choice for many services, or complete unavailability of certain services for Indian consumers.

- It is also stressed that the consumers should be allowed to exercise their 'right to choice' in case of storing data with an entity/location offering the best standard of security in safeguarding the rights of the consumer. Privacy of consumers should be an important facet of doing legitimate business within this space.

Security risk due to vulnerability of undersea cables

- It is advised that the same measure of analysis of security threats need to be looked into for housing data within the country as done for data moving outside. Also, there may not be a study conducted so far which can conclusively show that data localisation mandate enhances security and alleviates associated risks.

Security risks & preventing foreign surveillance

- This was touted to be a valid ground of mandating localisation. However, counter arguments of this view with respect to the possibility of enhanced mass surveillance by the local government also need to be kept in mind. CUTS' recommends the need to advocate for conducting a risk analysis in consultation with experts to determine the security risks of storing data outside the country or within the country.
- India is ranked 23rd among 165 nations in the UN ranking for cyber security index. This fact questions India's potential and preparedness in addressing cyber security risks while it considers housing the data within its geographical borders. Inadequacy of the number of cyber-security experts in the country also needs to be highlighted in this regard.

Impact on Industry

- It needs to be pointed out that data localisation may fuel concerns related to digital colonialism with smaller local players being left out. This was because the large foreign companies will be able to mobilise the requisite resources to invest in setting-up their Data Centres (DCs) within India, though the same may not be possible for smaller domestic companies. The possible enhanced costs of setting-up or renting such infrastructure along with the absence of cheaper foreign cloud services may dent their business interests. In addition, fears of large foreign businesses deciding not to serve India instead of getting into the hassle of data mirroring and exclusive storage (if required), must also be considered which may result in loss to consumers.
- Data Centres being at a nascent stage in India needs careful examination and could use regulatory sandboxes to avoid creating tremors and hampering future prospects with mandating hard data localisation. The legal procedures also have to be spelled out clearly to warrant access to data in a transparent manner having regard to due process of law.

As per the industry, and civil society and consumer groups, data localisation is more likely to be counterproductive not only to the interest of the consumers, but to the whole society. The argument also extended to question the basis of mandating data localisation as it does not meet the objectives, as stated in the Bill. It neither addresses the issue of safeguarding privacy nor does it add value in enhancing security.

Therefore, it is recommended that the regulation making process be more balanced and proactive, instead of being merely a reactive one. Regulations can have varied and divergent impacts on different stakeholders, and it is thus necessary to ensure that in the process of

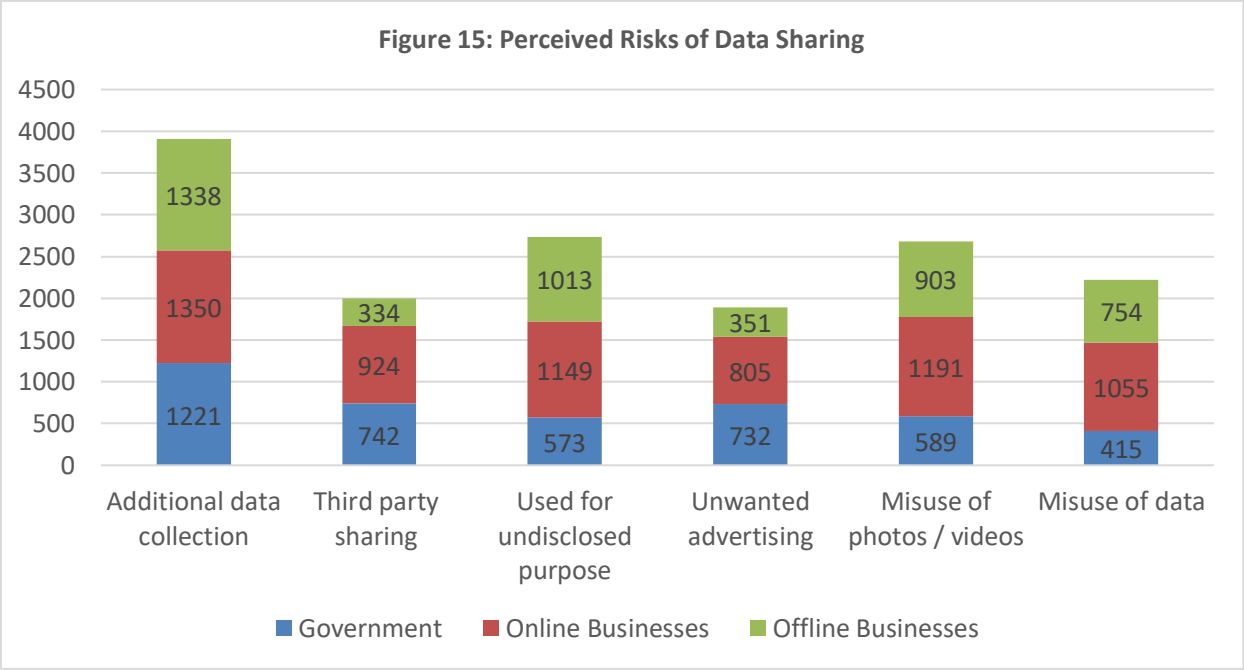
achieving its objectives, the costs imposed by regulation on stakeholders do not outweigh its benefits.

Moreover, assumptions and fear ought to be replaced with evidence-based research from various perspectives – economical as well as civil liberties. The observation of the committee must be treated as a recommendation, i.e. *India would have to carefully balance possible enforcement benefits of localisation with the costs involved in mandating such a policy in law*. Accordingly, undertaking RIA or CBA of the proposed data mirroring mandate becomes imperative in order to map its impact on various stakeholders before its enactment.

Purpose Limitation

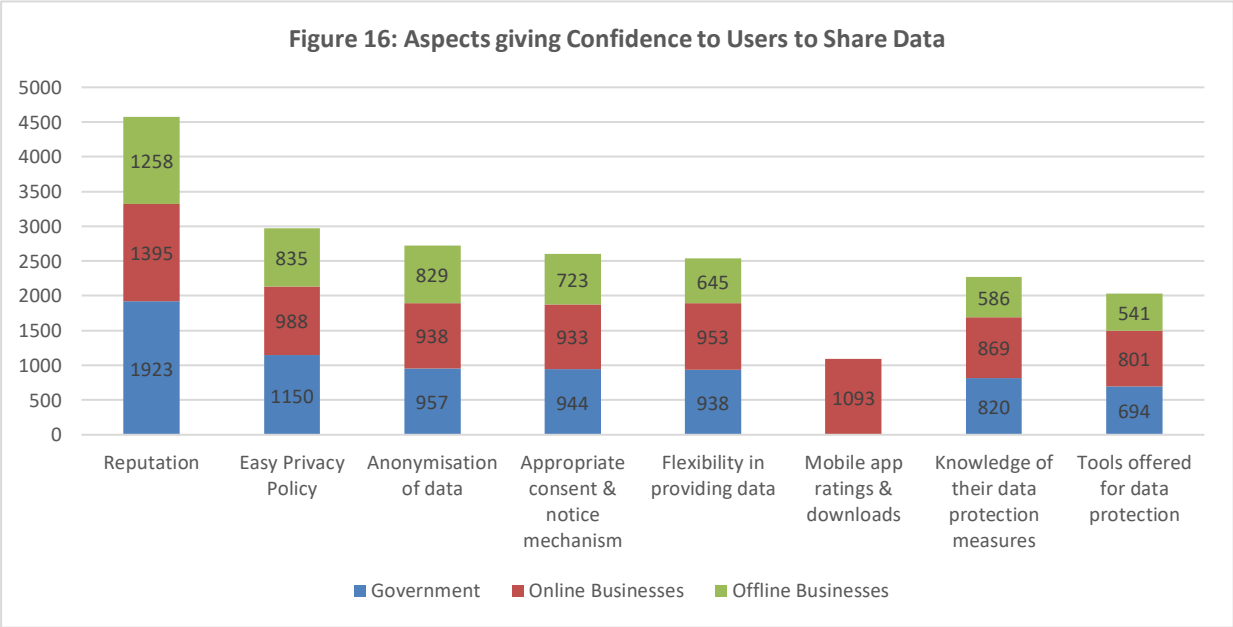
CUTS' user perception survey attempted to gauge the perception of users with respect to the purpose of data collection/ processing by the service providers. Most respondents felt that the data was being collected for targeted advertising. However, the least chosen option pertained to 'using the data for legitimate purpose'. Despite this, interestingly, most consumers expected that data fiduciaries should use the data only for the purpose of collection. Consequently, the introduction of purpose limitation in the Bill is laudable.

CUTS' user perception survey also delved into perceived risks by data principals in sharing of data with data fiduciaries. The fear of additional data collection, by data fiduciaries or data being used for undisclosed purposes, along with misuse of data for unauthorised purposes, were the most flagged risks, which reiterates the importance of purpose limitation in data collection/processing.



Data Audit and Data Trust Score

With respect to Sections 35(2) and 35(6) of the Bill, on assigning a rating in the form of a data trust score to various data fiduciaries, it is pertinent to examine issues users consider important, while deciding to share data. The factors include: reputation of the service provider; easy to read privacy policies; anonymisation of data; having appropriate consent and notice mechanisms; flexibility in providing data (providing limited data for availing limited service); number of mobile app ratings and number of downloads; knowledge of the data fiduciary's data protection measures; and tools offered for data protection.



In order to reduce the subjectivity in data audits and data trust scores, benchmarking the functioning of data fiduciaries to collaboratively developed personal data protection standards and best practices might be useful. A certification method would help data fiduciaries to verify their conformance to a visible badge of recognition ensuring transparency and accountability. This methodology could be adopted in the form of a Trustmark or Trust seals being used in Singapore,[15] and have been considered by several other foreign jurisdictions like EU,[16] Australia,[17] United States[18] as an indicator for sound data protection regimes. Such standards may be designed in a consultative and transparent manner by involving the industry players, consumer groups and other relevant stakeholders.

[15] https://www.pdpc.gov.sg/Organisations/Data-Protection-Trustmark
[16] https://gdpr-info.eu/art-42-gdpr/
[17] https://www.alrc.gov.au/publications/31.%20Cross-border%20Data%20Flows%20/trustmarks
[18]https://blog.trade.gov/2017/12/29/united-states-becomes-first-economy-to-offer-asia-pacific-economic-cooperation-privacy-trustmark-to-data-processors/

Consumer Grievance Redress Mechanism

The grievance redress mechanism in the Bill facilitates the consumer/data principal to exercise its right to redress but falls short of ensuring transparency and accountability, which could dampen the confidence and trust of the consumer in the system. There is a need to identify an effective and efficient process, which answers the preliminary questions like who to approach, how to approach, timeframe for adjudicating complaints. The process should enhance the confidence and trust of the users as it encourages them to avail of the system more frequently in effective and efficient manner.

The adjudicating wing within the Data Protection Authority is intended to be quasi-judicial body, while the Central government, which is a part of the executive, will prescribe the operation, segregation, independence and neutrality of the wing. There may be instances where the government is a party to a dispute. In such a case, there would be a conflict of interest as the government would be a party to the dispute before the adjudicating wing, and will also have the power to appoint members to the adjudicating wing. Thus, there is a need to amend 68(2) of the Bill to make the adjudicating wing truly independent. In this regard, principles laid down by the Financial Sector Legislative Reforms Commission and CUTS suggestions on the Regulatory Reform Bill may be taken into account.[19]

According to CUTS' user perception survey, at present, few respondents believed that they had experienced a data privacy violation. However, this might not present a correct picture with respect to data privacy violation and consumer grievance.

Based on CUTS experience of running a Consumer Care Centre (Grahak Suvidha Kendra, supported by Ministry of Consumer Affairs), it appears that the culture acknowledging violation of a consumer right/ existence of grievance and filing a complaint does not exist in the country.[20] Consequently, there is a need to generate awareness and built capacity among consumers with respect to grievance redress. There is also a need for creating consumer trust on complaint investigation and redress authorities.

To this end, the Bill should have a clear time frame for resolving complaints at every step of the process. Although a 30-day period has been marked for resolving the complaint at the data fiduciary level, no time frame has been stipulated for disposing the complaint from the level of the Data Protection Authority and onwards. The Bill could borrow a leaf from the recent Consumer Protection Bill, 2018 which assigns 21 days to decide the admissibility of the complaint from the date on which the complaint was filed. And if it is not decided within 21 days, the complaint is deemed to be accepted.

In addition, the Bill gives a miss to the opportunity of creating a new structure for adjudicating complaints. It chooses to rely on procedural laws like Civil Procedure Code, Criminal Procedure Code, etc., which are complex in nature and the process thereof requires

[19] http://www.cuts-ccier.org/event-Regulatory_Reforms_in_India-A_Roundtable.htm
[20] https://www.centerforfinancialinclusion.org/lessons-from-running-a-consumer-care-center-in-india/

assistance of a legal expert. This acts as an additional disincentive due to the associated costs and mental burden.

It is recommended that the processes adopted by the Data Protection Authority are simple and comprehensible to enable a data principal to take up its own matter. The regulator could provide regular updates to complainants on the progress of their complaint through a communication channel of their preference. Ultimately, the redress mechanism should be accessible, simple to use and should not prove to be burdensome for the consumer, offering them multiple channels to register complaints, such as toll-free calling lines, central online portal, email, letter, fax and even in person, which will also build up the regulators' visibility on firms' behaviour.

The Bill can also explore alternate dispute redress mechanisms, such as mediation and credible and experienced consumer organisations like CUTS can act as a mediator between data principal and data fiduciaries.[21]

It is proposed that a regulator should record all genuine complaints and enquiries in an open central complaint database, such as compliant redress mechanism of Securities and Exchange Board of India or SEBI (SCORES) or the insurance regulator. This database could be used to monitor progress on complaint resolution and, also as an analytical tool for researching vulnerabilities in the data economy. The database should be suitably anonymised and be compliant with the provisions of data protection regime.

Notification on Data Breach

The Bill should contain the obligation to notify data principals and the DPA of the breach concurrently. The data principal should be intimated about the breach irrespective of the assessment whether there exists a need to take an action on behalf of the data principal or whether the harm crossed the threshold limit of severity.

Need for Regulatory Impact Assessment

The Bill seems void of being a product of any evidence-backed/scientific research. The drafting of the Bill should have been preceded by adequate evidence-backed research to clearly identify the areas requiring attention, keeping in mind the interests of all stakeholders. Accordingly, CUTS' highly recommends the MeitY, to adopt and institutionalise undertaking RIA[22] and CIA, while framing/providing any suggestions on the policy, regulatory and/or legislative framework regarding 'Citizen Data Security and Privacy'.

RIA is a process of systematically identifying and assessing direct and indirect impacts of regulatory proposals and existing regulations, using consistent analytical methods. It involves a participatory approach via public consultation to assess such impact,

[21] http://www.cuts-international.org/cart/Grahak_Suvidha_Kendra.htm
[22] http://cuts-ccier.org/ria/

determination of costs and benefits, and selection the most appropriate regulatory alternative. Adopting such an approach will ensure framing of optimal regulations.

The adoption of RIA has also been recommended by various committees which have been highlighted in a CUTS paper[23], a version of which was also presented to the Better Regulatory Advisory Group (BRAG) which was constituted by the Department of Industrial Policy and Promotion (DIPP).

Phased Implementation of the Law

CUTS' recommends a phased implementation of the Bill. Currently, section 97 proposes all sections of the Draft Bill to be enforced within 18 months. However, given the significant impact that it would have on the entire economy the implementation of various aspects of the Bill should be carried out in a phased manner. Firstly, this would allow the industry to truly assess the impact of the Bill (when enacted as law) on their businesses and take appropriate measures for compliance. Also, as a majority of the standards under the Bill need to be enforced through subordinate legislation, this would allow the government to conduct meaningful discussions with the industry, civil society and other regulators to develop policy. It would also give time to develop a culture of privacy and build regulatory capacity to govern the data privacy framework for a country with a billion plus citizens.

CUTS' looks forward to assisting MeitY in its endeavours of securing citizens' personal data.

For any clarifications / further details, please feel free to contact Udai Mehta at usm@cuts.org +91 98292 85926.

****

[23] http://www.cuts-ccier.org/pdf/ViewPointPaper-Regulatory_Reforms_Needed_for_Ease_of_Doing_Business_in_India.pdf