Respondent Category

1. Subject Expert (i.e. those from civil society organisations, independent consultants and experts, lawyers, industry associations, consumer groups, government representative etc.) _____
2. Service Provider (i.e. those from businesses engaged in providing digital communication, entertainment, social media, financial and e-commerce services) ______

Sector (for service providers only)

1. Social Media
2. Communication
3. Entertainment
4. Finance
5. e-commerce
6. Others (please specify) ____________________

CUTS International

Questionnaire

Measuring the Impact of Data Localisation on Consumers

Disclaimer

Your responses would be kept strictly confidential and the anonymised and aggregated responses would be used for research purposes only.

For any queries or clarifications, please feel free to contact: Sidharth Narayan, Assistant Policy Analyst, CUTS International, at sid@cuts.org.

About the Questionnaire

Data Localisation (including Data Mirroring) has been mandated by various laws/regulations, such as the draft personal data protection bill, RBI notification on storage of payment systems data, draft eCommerce policy etc. Notably, the scope of data localisation varies in each of these regulations.

For subject experts, the scope of data localisation for the purpose of the study has been restricted to sections 40 and 41 of the Draft Personal Data Protection Bill 2018, which broadly mandate the following about **personal data**:

- Every data fiduciary shall ensure the storage, on a server or data centre located in India, of at least one serving copy of personal data to which the Act applies.

- The Central Government shall notify categories of personal data as critical personal data that shall only be processed in a server or data centre located in India.
- Personal data other than those categories of sensitive personal data notified as critical personal data may be transferred outside the territory of India, subject to certain conditions.
- Sensitive personal data notified by the Central Government may be transferred outside the territory of India, under certain circumstances.

We understand that services providers deal with a mix of non-personal, personal, sensitive personal and critical personal data their operations. Experts may use their judgement to determine the extent of applicability of localisation requirement on service providers, and fill the questionnaire from a consumer perspective. However, service providers may fill the questionnaire based on all the regulations applicable to them.

The questionnaire below, seeks to gauge your expert judgement on the following:

- The probable impact on consumers, with respect to the given parameters for data driven services in India (such as social media, e-commerce, entertainment etc.), post-DL. The same may be based on the following assumptions:
    - Currently, there is mostly free flow of data across borders, without any major propositions of data localisation, i.e. laws / regulations as on January 2018 are applicable.[1]
    - Data Localisation is set to come in the form of the draft personal data protection bill, and other sector specific regulations.
    - Ratings / scores on impact of data localisation may be given by you on a scale between -5 to +5, based on the assumption of the current position of each parameter in India being at 0 or neutral, i.e. the country being in a position of laws/regulations applicable on 1st January 2018.
- The reasons (open-ended) for the ratings given under each parameter for measuring the impact of DL.
- Self-ratings need to be done, based on self-evaluation of the level of expertise on the given parameters. These may be given on a scale of 1 to 5.
- Also, each of the given parameters would need to be rated on a scale of 1 to 5, with respect to their relative importance, while considering DL.

[1] Only the following laws / regulations are in force - Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, National Data Sharing and Accessibility Policy (NDSAP) of India 2012, National Security Council's (NSC) Paper on Data Localisation 2014, Indian Government's Guidelines for Government Departments for Contractual Terms related to Cloud Storage 2017

Q1. How will Data Localisation impact consumers, based on the below mentioned indicators, on a scale of -5 to +5, as per the description given below? You may give ratings in decimal points as well. Also, kindly give reasons for your response for each parameter.

Your responses would be normalised, during data analysis, based on your self-indicated level of expertise and weight provided to different parameters, as gauged in question 2.

Rating	Description	Rating	Description
0 = No impact			
-1	Negligibly Negative	+1	Negligibly Positive
-2	Somewhat Negative	+2	Somewhat Positive
-3	Moderately Negative	+3	Moderately Positive
-4	Very Negative	+4	Very Positive
-5	Extremely Negative	+5	Extremely Positive

S. No.	Parameters and Sub-Indicators	Change owing to DL (-5 to +5)
Parameter 1: What will be the impact of DL on availability of data driven services?		
1.1.1	Complete Availability of Services, i.e. number of features of a service being available in India, compared to the rest of the world. *Hypothetical Example*: communication services may continue to be available in India, but the video conferencing feature in it may not be available post DL.	
1.2.2	Number of services available in India. *Hypothetical Example*: certain services, such electronic transfer of remittances may altogether become unavailable to Indian consumers.	
Reason for Response		

S. No.	Parameters and Sub-Indicators	Change owing to DL (-5 to +5)
Parameter 2: What will be the impact of DL on cost of services for consumers?		
2.1.3	Free Services available in India, still remaining free. *Hypothetical Example*: services such as social media, communication continue to remain free for Indian consumers, post DL.	
2.2.4	Price of Paid Services, i.e. change in price of chargeable services. (higher score denoting lower prices) *Hypothetical Example*: subscription-based entertainment services are available at the same prices, as before DL.	

Reason for Response

S. No.	Parameters and Sub-Indicators	Change owing to DL (-5 to +5)
Parameter 3: What will be the impact of DL on quality of services?		
3.1.5	Reliability of Services, i.e. the probability that a service will perform its intended function adequately for a specified period of time, or will operate in a defined environment without failure. *Hypothetical Example*: accurate responses to queries will continue to show up in search engines, post DL.	
3.2.6	Ease of Engagement, i.e. the subtle aspects of the interface such as the design and readability of text, convenience and visual appeal of services. *Hypothetical Example*: browsing for products on e-commerce sites, will continue to be as convenient for consumers, as it is today, even after DL.	
3.3.7	Responsiveness to Consumers[2], such as number of drop-down options, time taken to execute consumer transactions etc. *Hypothetical Example*: quality of video calling remains	

[2] providing fast, friendly, knowledgeable service. https://yourbusiness.azcentral.com/customer-responsiveness-7789.html.

<table>
<tr><th>S. No.</th><th>Parameters and Sub-Indicators</th><th>Change owing to DL
(-5 to +5)</th></tr>
<tr><td></td><td>unchanged after DL.</td><td></td></tr>
<tr><td colspan="3"><b>Reason for Response</b></td></tr>
<tr><td colspan="3">Parameter 4: What will be the impact of DL on innovation?</td></tr>
<tr><td>4.1.8</td><td>Rate of Delivery of Updated Versions of Service
<i>Hypothetical Example</i>: frequency of mobile app updates, post DL.</td><td></td></tr>
<tr><td>4.2.9</td><td>Relevance and Quality of Updates, i.e. improvement of service after updates.
<i>Hypothetical Example</i>: improved quality of service, or new features being added in service offerings, post DL.</td><td></td></tr>
<tr><td>4.3.10</td><td>Domestic creation of emerging technologies & services, such as those dependent on artificial intelligence, blockchain etc.
<i>Hypothetical Example</i>: India’s rank improving in the Global Innovation Index, post DL.</td><td></td></tr>
<tr><td colspan="3"><b>Reason for Response</b></td></tr>
<tr><td colspan="3">Parameter 5: What will be the impact of DL on possible data breaches[3]?</td></tr>
<tr><td>5.1.11</td><td>Ability to Prevent Data Breaches.</td><td></td></tr>
</table>

[3] GDPR defines a “personal data breach” in Article 4(12) as: “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised. disclosure of, or access to, personal data transmitted, stored or otherwise processed”

S. No.	Parameters and Sub-Indicators	Change owing to DL (-5 to +5)
	Hypothetical Example: competency of service providers to prevent data breaches (whether by external hackers, or internal errors), post DL.	
5.2.12	Number of Data Breaches (lower score denoting more data breaches).	
5.3.13	Quality of Response to Data Breaches (higher score denoting better response to data breaches). *Hypothetical Example*: quicker and more effective response by service providers to mitigate impact of data breaches, post DL.	
Reason for Response		
Parameter 6: What will be the impact of DL on possible privacy violations[4]?		
6.1.14	Ability to Prevent Privacy Violation (higher score denoting better ability to prevent privacy violation). *Hypothetical Example*: extensive usage of principles of data anonymisation[5], preventing unauthorised data sharing with third parties etc., post DL.	
6.2.15	Number of Privacy Violations (lower score denoting more privacy violations)	
6.3.16	Number of requests by Law Enforcement Agencies (LEA) for access to Data, (lower score denoting more requests for access). *Hypothetical Example*: for the purpose of the study, a greater number of requests, denote increased risk of privacy violation.	

[4] The interference of a person's right to privacy by various means. https://thelawdictionary.org/violation-of-privacy/

[5] "Anonymisation" in relation to personal data, means the irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified. https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

S. No.	Parameters and Sub-Indicators	Change owing to DL (-5 to +5)
6.4.17	Risk of Surveillance by Indian Government[6] (lower score denoting higher risk of such surveillance).	
6.5.18	Quality of Response to Privacy Violations (higher score denoting better response to privacy violation). *Hypothetical Example*: quicker and more effective response by service providers to mitigate impact of privacy violation, post DL.	
6.6.19	Likelihood of availability of effective Privacy Protection Tools to Consumers, such as incognito mode, cookie blockers etc. (higher score denoting more tools being available).	
Reason for Response		
Parameter 7: What will be the impact of DL on possible cyber attacks[7]		
7.1.20	Ability to Prevent Cyber Attacks (higher score denoting better ability to prevent cyber-attacks). *Hypothetical Example*: extensive usage of digital security tools, in order to prevent cyber-attacks, post DL.	
7.2.21	Number of Cyber Attacks (lower score denoting more cyber-attacks)	
7.3.22	Quality of Response to Cyber Attacks (higher score denoting better response to cyber-attacks). *Hypothetical Example*: quicker and more effective response by service providers to mitigate impact of cyber-attacks, post DL.	
Reason for Response		

[6] A surveillance state is defined as a state which legally surveils all actions, locations, and friends of its citizens. https://piratetimes.net/what-is-a-surveillance-state-and-is-it-good-for-you/

[7] A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

S. No.	Parameters and Sub-Indicators	Change owing to DL (-5 to +5)
Parameter 8: What will be the impact of DL on consumer grievances?		
8.1.23	Number of Consumer Grievances[8], i.e. consumer suffering irrespective of being reported. (lower score denoting greater number of consumer grievances)	
8.2.24	Ability to Redress Consumer Grievances, i.e. ability of service providers to provide effective redressal to consumer complaints, number of complaint redressal mechanisms available to consumers etc. (higher score denoting better ability to redress consumer grievances)	
8.3.25	Consumer Grievance Redressal Avenues, i.e. number of complaint redressal mechanisms provided to consumers by service providers. (higher score denoting more consumer grievance redressal avenues)	
Reason for Response		
Parameter 9: What will be the impact of DL on freedom of speech and censorship?		
9.1.26	Freedom of speech and expression (lower score denoting increased obstruction and curtailment to free speech and expression). *Hypothetical Example*: excessive requests for takedown	

[8] May have six separate dimensions (timeliness, facilitation, redress, apology, credibility, and attentiveness) https://journals.sagepub.com/doi/10.1177/1094670502238917

<table>
<tr><th>S. No.</th><th>Parameters and Sub-Indicators</th><th>Change owing to DL (-5 to +5)</th></tr>
<tr><td></td><td>of content from search engines and/or social media sites, post DL.</td><td></td></tr>
<tr><td>9.2.27</td><td>State censorship (lower score denoting increased state censorship).
<em>Hypothetical Example</em>: excessive internet shutdowns, or suspension of certain services, post DL.</td><td></td></tr>
<tr><td colspan="3"><strong>Reason for Response</strong>
____
____
____
____
____________________</td></tr>
<tr><td colspan="3">Parameter 10: What will be the impact of DL on India’s national security[9]?</td></tr>
<tr><td>10.1.28</td><td>Likelihood of Surveillance by Foreign State[10] (higher score denoting lower likelihood of such surveillance).</td><td></td></tr>
<tr><td>10.2.29</td><td>Surveillance by Foreign Non-State Actors[11] (higher score denoting lower likelihood of such surveillance).</td><td></td></tr>
<tr><td>10.3.30</td><td>Risk to critical infrastructure, or strategic national cyber assets. (lower score denoting more risk to critical infrastructure).</td><td></td></tr>
<tr><td>10.4.31</td><td>Ability to lawfully intercept data required for a pre-emptive response to a national security threat (higher score denoting better ability).</td><td></td></tr>
<tr><td colspan="3"><strong>Reason for Response</strong>
____________________</td></tr>
</table>

[9] A country's national security is its ability to protect itself from the threat of violence or attack. https://www.collinsdictionary.com/dictionary/english/national-security

[10] capture peacetime surveillance by one state of the communications of another state’s officials or citizens who are located outside the surveilling state’s territory, using electronic means such as Internet and cell phone monitoring or satellites. http://www.oxfordscholarship.com/view/10.1093/oso/9780190685515.001.0001/oso-9780190685515-chapter-18

[11] Consumer surveillance is the monitoring and recording of people’s activities and data, for commercial purposes https://whatis.techtarget.com/definition/consumer-surveillance

S. No.	Parameters and Sub-Indicators	Change owing to DL (-5 to +5)
Parameter 11: What will be the impact of DL on LEAs possible access to data?		
11.1.32	Number of Responses to LEA Requests (higher score denoting more requests being responded to).	
11.2.33	Likelihood of apprehending cyber criminals.	
11.3.34	Likelihood of gathering due evidence for prosecuting cyber criminals.	
Reason for Response		
Parameter 12: What will be the impact of DL on India's economic development?		
12.1.35	Generating employment in IT/ITES sector, data storage, cloud services, data processing etc & other related sectors.	
12.2.36	Creating local Infrastructure in Telecom, Cloud Computing & other related areas	
12.3.37	Development of Local Businesses in Software, OTT Services, Cloud Computing, Artificial Intelligence etc.	
Reason for Response		

S. No.	Parameters and Sub-Indicators	Change owing to DL (-5 to +5)
Parameter 13: What will be the impact of DL on competition amongst service providers?		
13.1.38	Competition amongst service providers, whether domestic or foreign.	
13.2.39	Indian industry players competing with foreign service providers, i.e. Indian players getting a level-playing field post DL.	

Reason for Response

Q2. Please rate the given parameters with respect to their relative importance, while considering Data Localisation (5 = most important, and 1 = least important). Also, kindly give self-ratings on a scale of 1 to 5, based on a self-evaluation of your level of expertise in each of the given parameters. Please refer the table below for details. Both of these would be used to aggregate and normalise your responses at a parameter level.

Rating	Significance	Description
1	Fundamental Awareness (basic knowledge)	You have common knowledge or a basic understanding of the parameter.
2	Novice (limited experience)	You have limited experience on the parameter, and need help when analysing the same.
3	Intermediate (practical application)	You have functional competency to judge the parameter. Help from an expert may be required from time to time, but you usually use your judgement independently.
4	Advanced (applied theory)	You have applied knowledge on the parameter, and can apply your judgement without assistance. You are the recognised 'go to person' within your organisation on the parameter.
5	Expert (recognized authority)	You are known as an expert in this area, and can provide guidance to others, on the said parameter.

Parameter	Rating of Importance for Data Localisation (5 = most important, and 1 = least important)	Self-Rating (5 = expert, and 1 = fundamental awareness)
Availability of Service		
Quality of Service		
Cost of Service		
Innovation		
Data Breaches		
Privacy Violations		
Cyber Attacks		
Grievance Redress		
Freedom of Speech and Censorship		
National Security		
Law Enforcement Agencies Access to Data		
Economic Development		
Competition amongst Service Providers		

Q3. Overall, do you think Data Localisation will have a positive or negative impact on Indian consumers, based on the parameters mentioned above?

Indicators	Impact (-5 to +5)
General consumer welfare in availing digital technology driven services	

Q4. Assuming that Data Localisation is likely to be introduced, how do you suggest mitigating its negative impact, with respect to parameters on which you think consumers will be negatively impacted? You may choose (by circling) multiple options.

1. Implementing appropriate regulation to facilitate competition, innovation, standard setting, security and accountability among service providers in the market
2. Implementing appropriate regulation to ensure adequate checks and balances on government use of discretion and enhance accountability
3. Strengthen the proposed Data Protection Authority (DPA – under the draft personal data protection bill 2018), to reduce information asymmetry, ensure compliance and penalise non-compliance
4. Provide fiscal incentives/subsidies to foreign start-ups and MSMEs for local data storage.
5. Provide fiscal incentives/subsidies to domestic start-ups and MSMEs for local data storage.
6. Build domestic capacity of cyber-security experts, data centre management personnel, software experts etc.
7. Invest in developing requisite infrastructure for data centres in India.
8. Developing baseline principles for protecting consumers in digital economy sectors where data localisation is mandated
9. Others ____

Q5. Any other remarks or thoughts on Data Localisation, from a consumer's perspective?

____

____

____

____

____

Please provide following details. We confirm that your details will be kept strictly confidential and will be utilised only for reaching out to you in case of queries or clarifications required on your responses.

Name: ________________________________

Organisation: ____________________________

Designation: ____________________________

Mobile: ________________________________

E-Mail ID: ______________________________

Signature: ______________________________

Please let us know if you would be comfortable in being acknowledged (only your name, and not your responses) in the research outputs for the study.

1. Yes

2. No

Disclaimer

Your responses would be kept strictly confidential and the anonymised / aggregated responses would be used for research purposes only. Your views shall only be made public upon receiving your express written consent.

Important Terms

Personal Data: Draft Personal Data Protection Bill defines personal data as 'data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information'.

Sensitive Personal Data: Draft Personal Data Protection Bill defines sensitive personal data as 'personal data revealing, related to, or constituting, as may be applicable — (i) passwords; (ii) financial data; (iii) health data; (iv) official identifier; (v) sex life; (vi) sexual orientation; (vii) biometric data; (viii) genetic data; (ix) transgender status; (x) intersex status; (xi) caste or tribe; (xii) religious or political belief or affiliation; or (xiii) any other category of data specified by the Authority under section 22'.

National Security: A country's national security is its ability to protect itself from the threat of violence or attack.[12]

Surveillance by Foreign State: capture peacetime surveillance by one state of the communications of another state's officials or citizens who are located outside the surveilling state's territory, using electronic means such as Internet and cell phone monitoring or satellites.[13]

Surveillance by Foreign Non-State Actors: Consumer surveillance is the monitoring and recording of people's activities and data, for commercial purposes by entities other than state.[14]

Data Breach: GDPR defines a "personal data breach" in Article 4(12) as: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"

Privacy Violation: The interference of a person's right to privacy by various means.[15]

Cyber-Attack: A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization.[16]

Difference Between Data Breach, Privacy Violation and Cyber-Attack

[12] https://www.collinsdictionary.com/dictionary/english/national-security

[13] http://www.oxfordscholarship.com/view/10.1093/oso/9780190685515.001.0001/oso-9780190685515-chapter-18

[14] https://whatis.techtarget.com/definition/consumer-surveillance

[15] https://thelawdictionary.org/violation-of-privacy/

[16] https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Parameters	Data Breach (largely unintentional by data fiduciary)	Privacy Violation (largely intentional by data fiduciary)	Cyber-Attack (by third party)
Definition	GDPR defines a "personal data breach" in Article 4(12) as: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"	The interference of a person's right to privacy by various means.[17]	A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization.[18]
Reason for occurrence	Data can be breached by internal faults, as well as external elements.	Privacy violation can be caused due to internal errors, and /or intentional misuse.	Cyber-attacks are not limited to harm to database, but can result in disruption or blocked access to services.
Example	Data leakage due to technical faults.	Misappropriation of data, by unauthorised third-party sharing.	Deliberate attempt of malicious third parties, hacking service providers application to disrupt services.

[17] https://thelawdictionary.org/violation-of-privacy/

[18] https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html