International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 09 | Sept - 2021 ISSN: 2582-3930

AN EXPLORATORY STUDY ON DATA LOCALISATION AND ITS INFLUENCE ON E-COMMERCE IN INDIA

Sub Theme: Digitalization, Economic Policies for Trade Facilitation

Dr. Rutupurna Dash

ABSTRACT:

Data localisation, which entails companies to store data in local servers and not in another country or jurisdiction if they collected from individuals live in those countries. According to the UNCTAD's 'Digital Economy Report 2019', e-commerce has generated a total business of 28 lakh crore Rupeesin 2017,this volume took India to ninth-highest e-commerce sales globally in the same year,this included goods and services sold online, transactions via platform-based companies such as ride-hailing apps and room-sharing platforms, contributing 15% to India's GDP.The only way for developing countries to own and control data generated in their territories is by restricting the cross-border flows of important personal and community data. The UNCTAD's 'Digital Economy Report 2019' says "The only way for developing countries to exercise effective economic "ownership" of and control over the data generated in their territories may be to restrict cross-border flows of important personal and community data".Till now the multinational companies are managed to take data and used to store them in foreign servers exposing the local population to live under the concern of personal data theft.RBI has made data localisation mandatory for payment systems, disallowing sharing of the data with a third-party. This research paper is an attempt to find out the possible outcomes of data localisation and how this will have a greater influence on the E-commerce business. Simple OLS regression result is used for the study. It is observed from the study that the localisation of data storing will though increase the cost of operation for the multinational players but will not have significant impact on the E-commerce business.

Keywords:*Data localisation; E-commerce; local population; multinational companies; developing country*

Introduction:

When a customer swipes its Visa card or use Amazon's services, no wonder the customer's financial and personal information is carried, processed or stored in a server located outside the Indian territory. Well, most of the data tend to be either partly or completely stored outside India. Quite apart from worries about who has access to these data overseas, the Indian government and regulators too have limited access to this data. This is what the RBI wants to change through its data localisation rules. Earlier in October 2018 companies from around the world scrambled to comply with the RBI's deadline for localisation of all sensitive data belonging to Indian users of various digital payment services. Data localisation is the act of storing data on any device physically present within the borders of a country. As of now, most of these data are stored, in a cloud, outside India. RBI's diktat has followed the draft data protection law recommended by Srikrishna committee in July/August 2018. One of the recommendations was that the government must enjoy unfettered access to its citizens' or residents' data for use in domestic policy-making (through Big Data analytics and Artificial Intelligence). Thus, to sum it up data localization is the act of storing data on any device that is physically present within the borders of a specific country where the data was generated. Free flow of digital data, especially data which could impact government operations or operations in a region, is restricted by some governments. The requirements for data localization can be for different reasons, such as mandate by national laws that require certain data to be physically stored on servers within the country or the need to comply with data protection regulations. This is especially true when it comes to cross-border transfers in which case data storage within a country seems to be a cost effective and better solution, or in cases where enterprise customers of data storage technologies and public opinion favours in-country data-storage solutions and strategies.

Theoretical Overview:

Localisation mandates that companies collecting critical data about consumers must store and process them within the borders of the country. The RBI had issued a circular mandating that payments-related data collected by payments providers must be stored only in India, setting an October 15 deadline for compliance. This covered not only card payment services by Visa and MasterCard but also of companies such as Paytm, WhatsApp and Google which offer electronic or digital payment services. Many companies are yet to comply with this rule and the RBI has not specified any fines or penalties for the delay.Why is it important?

The main intent behind data localisation is to protect the personal and financial information of the country's citizens and residents from foreign surveillance and give local governments and regulators the jurisdiction to call for the data when required. This aspect has gained importance after a spate of lynchings

across States was linked to WhatsApp rumour. Revelations of social media giant Facebook sharing user data with Cambridge Analytica, which is alleged to have influenced voting outcomes, have led to a global clamour by governments for data localisation.Data localization often requires better IT infrastructure and stringent security measures for data related to business operations. Many attempt to protect and promote security across borders, and therefore encourage data localization. While some arguments support data localization, some feel that misguided policies on data localization could cause serious harmful consequences to citizens and economies alike.

The other argument is that data localisation is essential to national security. Storing of data locally is expected to help law-enforcement agencies to access information that is needed for the detection of a crime or to gather evidence. Where data is not localised, the agencies need to rely on mutual legal assistance treaties (MLATs) to obtain access, delaying investigations. On-shoring global data could also create domestic jobs and skills in data storage and analytics too, as the Srikrishna report had pointed out.However, on the flip side, maintaining multiple local data centres may entail significant investments in infrastructure and higher costs for global companies, which is why they seem to be up in arms against these rules.

As all of us are trusting global service providers with more and more information, both on a voluntary and involuntary basis, we may like to have greater accountability from these firms about the end-use of this data. Data localisation may not entirely avoid Facebook-Cambridge Analytica-like episodes but it may at least ensure that domestic law enforcement can respond more effectively to our complaints.The bottom line is that India has a stronger bargaining chip than most nations in pushing for data localisation access to its billion-strong consumer market.Some favour data localization due to fear of losing private data to hackers in the case of foreign data storage solutions. Some oppose data localization, as it is seen as hindering the flexibility of the internet.

Literature Review:

Requirements for local storage and processing of data are commonly referred to as ‘data localization’ or ‘data residency’ requirements. Data localisation can broadly be defined as 'any legal limitation on data moving globally and compelling it to remain locally.[1]These policies can take a variety of forms. This could include a specific requirement to locally store copies of data, local content production requirements, or imposing conditions on cross border data transfers that in effect act as a localization mandate.[2]Policies that seek to

[1]Joshua Meltzer, ‘The Internet, Cross-Border Data Flows and International Trade’ [2013] Issues inTechnology Innovation 16 https://www.brookings.edu/wp-content/uploads/2016/06/internet-dataandtrade-meltzer.pdf.

[2]For instance, some countries, such as Malaysia, permit transfers only with the explicit consent of the data subject. In some cases, this can serve as a significant impediment.

ensure domestic control over data have been termed as 'data nationalism'.[3]'Data exceptionalism' is a school of thought that argues that data is un-territorial and therefore incompatible with existing concepts of territorial jurisdiction.[4]However, there are a number of scholars who have opposed 'data exceptionalism' and argue that territorial jurisdiction can be asserted over data.[5] The assertion of territoriality is the building blocks for any argument justifying data localisation.

Data nationalism' is a framing device that refers to the broader trend of countries asserting the primacy of national priorities (related to law enforcement, privacy, security, etc) over the vision of a global internet.[6] 'Data protectionism' is a manifestation of data nationalism may indicate imposing restrictions on cross-border transfers of data as a matter of economic policy.[7]Mandating local storage of data can be an element of such an agenda. 'Data sovereignty' is a connected phrase-which basically is a guarantee towards ensuring that national law applies to data even if it is outside of a nation's territory.[8] Other scholars have alternate understandings of data sovereignty, which necessarily entail keeping data within national territories.[9] 'Data colonialism' is another term that has been used widely in India and other countries to justify data localisation. Broadly, an understanding of 'Data colonialism' refers the extractive practices of modern day western digital companies through data-driven revenue generation and behavioural modification, which are analogous to predatory colonial practices of the past.[10]

Therefore, Basu, A. et. al (2019) has of opinion that the manner in which a localisation gambit is enforced will determine how it fits into the apparatus of data nationalism. The goal should be to further 'data sovereignty' without engaging in excessive 'protectionism' such that India can assert it's laws without falling foul of diplomatic or legal agreements with foreign stakeholders.The digital population in ASEAN is on the rise. As

[3] See for instance: Anupam Chander, Uyên P. Lê, Data Nationalism, 64 Emory L.J. 677 (2015), http://law.emory.edu/elj/content/volume-64/issue-3/articles/data-nationalism.html;
D. Castro, The False Promise of Data Nationalism, December 2013, <http://www2.itif.org/2013-false-promise-data-nationalism.pdf>;
C. Kuner, Data Nationalism And Its Discontents, Emory Law Journal, 2015 https://brusselsprivacyhub.eu/onewebmedia/kuner.pdf.
[4]See,for example Zachary D. Clopton, Territoriality, Technology, and National Security, 83 U. CHI.L.REV. 45 (2016)
[5] A.Woods, Against Data Exceptionalism, Stanford Law Review, 2016 https://uknowledge.uky.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1593&context=law_facpub
[6] C. Kuner, Data Nationalism and Its Discontents, Emory Law Journal, 2015 https://brusselsprivacyhub.eu/onewebmedia/kuner.pdf
[7] M.F. Ferracane, E. Marel, The Cost of Data Protectionism, October 2018, http://ecipe.org/blog/the-cost-of-data-protectionism/
[8] C. Chelliah, With Data Sovereignty, Location Isn't Everything, https://www.oracle.com/uk/cloud/paas/features/data-sovereignty/
[9] J Labour, Data sovereignty: What you need to know and why you should care, 24 January 2018 https://cira.ca/blog/state-internet/data-sovereignty-what-you-need-know-and-why-you-should-care
[10] Couldry, Nick and Mejias, Ulises (2018) Data colonialism: rethinking big data's relation to the contemporary subject. Television and New Media. ISSN 1527-4764

of 2016, the world's Internet users amounted to more than 3.4 billion; most of them are located in Asia-Pacific.[11]Southeast Asia alone accounts for over 339 million of the digital population and has around 306 million active social media users, and these numbers are set to increase.[12]Data localization may have broader ramifications for the lives of a huge digital population, business operations and government functions in ASEAN. Normatively, there are two interlocking implications. First, regionally, ASEAN members' approaches to controlling data transfer, either individually or collectively, have a direct bearing on the full realization of the potentials envisaged by the AEC Blueprint 2025.[13] Also, their regulatory approach may have implications for the shaping of the international economic order. Many ASEAN members have been actively participating in recent mega regionalism, notably, the TPP and the RCEP. Presumably, given the formidable power of these combined markets, these initiatives may spill over into other fora and serve as a template on digital trade governance. The developments of new laws or policies on data flows both within and outside ASEAN would be a dynamic, usually reinforcing process that deserves consideration.[14]

The earliest efforts to control data flows date back to the 1970s.[15]Such efforts gained new momentum after Edward Snowden's leaks, which intensified debates on the limits of intelligence operations and set off the alarm for privacy and data protection.[16]Governments around the globe have been called upon to take what measures they see fit to rebuild trust in the online environment. Rightly or wrongly, one way to achieve this is to prohibit data from "travelling through the territory or infrastructure of 'untrustworthy' nations."[17]Today, over a dozen governments in developed and developing worlds – including some ASEAN members – have or are contemplating relevant policies.[18]These measures vary in terms of objectives, scope and enforcement, which may be roughly grouped into three types, as detailed below.[19]Governments in this camp take the strictest stance by requiring data to be stored in facilities physically located within a geographic border. Given

[11] See Internet Users in the World, Internet Live Stats, www.internetlivestats.com/internetusers/#byregion (last visited Dec. 29, 2017).
[12] Simon Kemp, The Full Guide to Southeast Asia's Digital Landscape, TechinAsia, Feb. 8, 2017, www.techinasia.com/talk/full-guide-southeast-asia-digital-landscape-2017 (last visited Dec. 29, 2017).
[13] See infra 50 and accompanying text.
[14] Han-wei liu, Data Localization and Digital Trade Barriers:ASEAN in Megaregionalism, 371-391, (2018) https://www.researchgate.net/publication/332059133
[15] Christopher Kuner, Transborder Data Flows and Data Protection Law 26–7 (2013); Allan Gotlieb et al., The Transborder Transfer of Information by Communications and Computer Systems: Issues and Approached to Guiding Principles, 68 Am. J. Int'l L. 227, 246 (1974).
[16]Scott Shane, Ex-Contractor Is Charged in Leaks on N.S.A. Surveillance, N.Y. Times,June 21, 2013, www.nytimes.com/2013/06/22/us/snowden-espionage-act.html? mcubz=1 (last visited Dec. 29, 2017).
[17] Jonah Force Hill, The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders, Lawfare Research Paper
Series 3 (2014), https://lawfare.s3-us-west-2.amazonaws.com/staging/Lawfare-ResearchPaper-Series-Vol2 No3.
[18]Anupam Chander & Uyên P. Lê, Data Nationalism, 64 Emory L. J 677 (2015).
[19]Shin-Yi Peng& Han-Wei Liu, The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?, 51 J. World Trade 183, 190 (2017).

its implications for the RCEP and thus ASEAN members, China's measures are of particular significance here. Long before the passage of its Cybersecurity Law,[20] China has addressed cross-border data flow in a relatively piecemeal fashion with several laws on overarching issues (e.g., Law on Guarding State Secrets, which generally prohibits data from leaving China if it is deemed to comprise "state secrets")[21] and numerous sector-specific regulations on trans-border data transfer.[22]

A more full-fledged framework on data transfer can be found in, among others, Article 37 of the Cybersecurity Law, which requires "personal information" and "other important data" collected or generated in mainland China by "critical information infrastructure operators" (CII operators) to be stored within the country's borders.[23]The terms "other information" and "CII operators" are given a rather broad scope. The former refers to "all kinds of information that, recorded electronically or through other means and taken alone or together with other information, is sufficient to identify a natural person's identity."[24]The latter would, per the draft "Critical Information Infrastructure Security Protection Regulations," cover any business operating in public communication and information services, finance, public services, energy, water resources, transportation, electronic communications and others. Worse, such local data storage mandates may arguably have no exemption for data about foreigners and overseas companies.[25]

Research Gap:

This research paper is the reflection of the Data Localisation and its Influence on E-Commerce in India. Yet no research has been conducted to find out the influence of data localisation on E-Commerce. This research has found out the gap related to the various emotional and financial benefits the Indian consumers and the business will get once the data localisation will take place.

Research Methodology:

In this research the attempt has been made to test the influence of data localisation on the consumers and the individuals involved in online business. In this research five assumptions were taken and the three close ended questions were asked to the participants grouped under two broad heads one is the consumers and the second

[20]Cybersecurity Law of the People's Republic of China (promulgated by the Standing Committee of the National People's Congress, Nov. 7, 2016, effective June 1, 2017).
[21]The Law of the People's Republic of China on Guarding State Secrets (promulgated by the Standing Committee of the National People's Congress, Sept. 5, 1998, as amended on Apr. 29, 2010).
[22]See e.g., Notice to Urge Banking Financial Institutions to Protect Personal Information (promulgated by the People's Bank of China, Jan. 20, 2011).
[23]Cybersecurity Law, supra note 11, art. 37.
[24]Id., art. 76.
[25]Graham Greenleaf & Scott Livingston, China's New Cybersecurity Law – Also a Data Privacy Law?, 144 Privacy Laws & Bus. Int'l Rep. 1-7 (2017).

is the online business owners. These five assumptions were based on Justice B.N.Srikrishna committee report stated as follows;

The notice and choice framework to secure an individual's consent is the bulwark on which data processing practices in the digital economy are founded. It is based on the philosophically significant act of an individual providing consent for certain actions pertaining to her data.[26]Consent has been viewed as an expression of a person's autonomy or control, which has the consequence of allowing another person to legally disclaim liability for acts which have been consented to.[27] This is enabled through notice - an affirmative obligation placed upon data fiduciaries to communicate the terms of consent.[28]A preponderance of evidence points to the fact that the operation of notice and consent on the internet today is broken.[29]Consent forms are complex and often boilerplate. Consequently,individuals do not read them; even if they attempt to, they might not understand them; even if they understand them, provisions to give meaningful consent in a granular fashion are absent.[30]Any enumeration of a consent framework must be based on this salient realisation:on the internet today, consent does not work. Towards ensuring that the consent to provide personal data more informed and meaningful, the committee pointed out the revised notice and choice framework need to be modified and designed to make data fiduciaries communicate the terms of consent to data principals in a clear form with substantive defined obligations. The committee was not clear about the standard of clarity that might be required in communicating consent. They have of opinion that the EU GDPR mandates that the consent must be freely given, specific, informed and unambiguous for processing of personal data. Since consent is prominently considered method of data collection, for validity of consent;the committee recommended the collection of data must be based on the following five principles i.e. 1) free, 2) informed, 3) clear, 4) specific and 5) capable of being withdrawn.

The questions were asked to the respondents based on the above five parameters to test following three hypotheses:

[26]Ryan M. Calo, Against Notice Skepticism in Privacy (and Elsewhere), 87(3) Notre Dame Law Review (2012) at p. 1049; Per Sanjay Kishan Kaul, J., in Puttaswamy, (2017) 10 SCALE 1 at p. 30 referring to the Second Circuit's decision in Haelan Laboratories v. Topps Chewing Gum. 202 F.2d 866 (2d Cir. 1953) penned by Judge Jerome Frank.

[27] Adam Moore, Toward Informational Privacy Rights, 44 San Diego Law Review (2007) at p. 812; Anita L.Allen, Why privacy isn't everything: Feminist reflections on personal accountability (Rowman & Littlefield, 2003) at pp. 115-16; John Kleinig, The Nature of Consent in The Ethics of Consent- Theory and Practice (Alan
Wertheimer and Franklin Miller (eds.), Oxford University Press, 2009) at p. 4.

[28]Ryan M. Calo, Against Notice Skepticism in Privacy (and Elsewhere), 87(3) Notre Dame Law Review (2012) at p. 1031.

[29]Ryan M. Calo, Against Notice Skepticism in Privacy (and Elsewhere), 87(3) Notre Dame Law Review (2012) at p.1031; Reidenberg et al, Privacy Harms and the effectiveness of the Notice and Choice Framework, 11(2) Journal of Law and Policy for the Information Society (2015); Florian Schaub et al, A design space for effective Privacy Notices (Symposium on usable privacy and security, 2015) at p. 2; LF Cranor, Necessary but not sufficient: Standardized mechanisms for privacy notice and choice, 10 Journal on Telecommunications and High Technology Law (2012) at p. 273.

[30]See B. W. Schermer et al, The crisis of consent: how stronger legal protection may lead to weaker consent in data protection, 16(2) Ethics and Information Technology (2014).

H_1: The users' Education level significantly differs the end users in disclosing their personal data.

H_2: The users' urgency level for consumption significantly differs in disclosing their personal data.

H_3:The users' geographical location significantly differentiates in disclosing their personal data.

Findings and Discussion:

To test the above mentioned three Hypotheses ANOVA test was utilised and the results are as follows

Hypothesis-1: The users' Education level significantly differs the end users in disclosing their personal data.

H_0: *The users' Education leveldoes not significantly differ the end users in disclosing their personal data.*

H_1: *The users' Education level significantly differ the end users in disclosing their personal data.*

validity of consent	Education level					Total
	Under Metric	Intermediate	Graduate	Postgraduate	Professional	
Free	4	13	16	13	8	54
Informed	9	11	17	22	10	69
Clear	8	11	19	20	18	76
Specific	4	16	26	22	19	87
Capable of Being Withdrawn	5	9	11	14	17	56
Total	30	60	89	91	72	342

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
Under Metric	5	30	6	5.5
Intermediate	5	60	12	7
Graduate	5	89	17.8	29.7
Postgraduate	5	91	18.2	19.2
Professional	5	72	14.4	25.3

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	498.64	4	124.66	7.189158	0.00093	2.866081
Within Groups	346.8	20	17.34			

From the above ANOVA table, it was evident that the F value is more than the F criticalvale i.e. 7.199>2.866. Hence as per the result the null hypothesis will be rejected. If again the p-value to be considered it shows that the calculated p value i.e. 0.000<0.05. Hence the Null Hypothesis will be rejected, i.e. the statement "The

users' Education level does notsignificantly differ the end users in disclosing their personal data". Hence to accept the alternate hypothesis i.e. The users' Education level significantly differs the end users in disclosing their personal data.

Hypothesis-2: The users' urgency level for consumption significantly differs in disclosing their personal data.

H_0:*The users' urgency level for consumption does not significantly differs in disclosing their personal data.*

H_1: *The users' urgency level for consumption significantly differs in disclosing their personal data.*

Validity of Consent	Urgency level				Total
	Highly urgent	Urgent	indifferent	not urgent	
Free	**9**	**13**	**18**	**14**	**54**
Informed	**14**	**17**	**17**	**24**	**72**
Clear	**16**	**21**	**21**	**21**	**79**
Specific	**8**	**26**	**27**	**27**	**88**
Capable of Being Withdrawn	**11**	**12**	**11**	**15**	**49**
Total	**58**	**89**	**94**	**101**	**342**

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
Highly urgent	5	58	11.6	11.3
Urgent	5	89	17.8	33.7
indifferent	5	94	18.8	34.2
not urgent	5	101	20.2	31.7

ANOVA Table

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	216.2	3	72.06667	2.599339	0.08813	3.238872
Within Groups	443.6	16	27.725			
Total	659.8	19				

From the above ANOVA table, it was evident that the F value is less than the F criticalvale i.e. 2.599<3.239. Hence as per the result the null hypothesis will be accepted. If again the p-value to be considered it shows that the calculated p value i.e. 0.088>0.05. Hence the Null Hypothesis will be accepted, i.e. the statement "*The users' urgency level for consumption does not significantly differs in disclosing their personal data*". Hence to

reject the alternate hypothesis i.e. *The users' urgency level for consumption significantly differs in disclosing their personal data*.

Hypothesis-3: The users' geographical location significantly differentiates in disclosing their personal data.

H_0:The users' geographical location does not significantly differentiate in disclosing their personal data.

H_1:The users' geographical location significantly differentiates in disclosing their personal data.

validity of consent	Urgency level			Total
	Urban	Semi-urban	Rural	
Free	28	22	29	**79**
Informed	24	27	19	**70**
Clear	22	23	21	**66**
Specific	17	21	33	**71**
Capable of Being Withdrawn	21	17	18	**56**
Total	**112**	**110**	**120**	**342**

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
Urban	5	112	22.4	16.3
Semi-urban	5	110	22	13
Rural	5	120	24	44

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	11.2	2	5.6	0.229195	0.798575	3.885294
Within Groups	293.2	12	24.43333			
Total	304.4	14				

From the above ANOVA table, it was evident that the F value is less than the F criticalvale i.e. 0.229<3.886. Hence as per the result the null hypothesis will be accepted. If again the p-value to be considered it shows that the calculated p value is greater than the alpha value i.e. 0.798>0.05. Hence the Null Hypothesis will be accepted, i.e. the statement "The users' geographical location does not significantly differentiate in disclosing their personal data". Hence to reject the alternate hypothesis i.e. The users' geographical location significantly differentiates in disclosing their personal data.

Result:

SL. NO	Hypothesis	Test Statistics	Finding	Result
1	The users' Education level does not significantly differ the end users in disclosing their personal data.	ANOVA	7.199>2.866	Rejected
2	The users' urgency level for consumption does not significantly differs in disclosing their personal data.	ANOVA	2.599<3.239	Accepted
3	The users' geographical location does not significantly differentiate in disclosing their personal data.	ANOVA	0.229<3.886	Accepted

Theoretical Implications:

The present topic is very new to India and still there are very few researchers are engaged in finding out theimpact of data localisation on online business and consumers. Since the primary information is not sufficiently available the research process becomes mundane. Again the negative after effect of data theft is still not publicly available in large quantity it is the researchers and the academicians need to continuously work on finding out the effect of data localisation on different stake holders.

Managerial Implications:

Since the government India has given more stress on digitalisation of business and governance there is a greater chance for data piration i.e. the personal information of citizens is revealed to outsider of live away from India. This brings in breach in privacy. If this information will be localised the operation cost for the data storing companies will increase and it directly or indirectly put pressure on the costing of the products. The decision of RBI for data localisation of financial information of Indians will definitely curb the international hacking problems.

Conclusion:

The results show that the impact of data localisation still not felt by both the consumers and the people involved in online business. Since there is a strong security concern from various security agencies the government has taken its first step to localise the data and has asked the companies involved in data gathering to store these data in the servers located in India. Again since this is the new topic and emerging area it was observed that the respondents were not aware of these cases, because of which there were to be elaborated before asking them the questions about their idea of disclosure of their personal information and the importance of cautious approach in revealing their personal and financial information.

References:

- Joshua Meltzer, 'The Internet, Cross-Border Data Flows and International Trade' [2013] Issues in Technology Innovation. https://www.brookings.edu/wp-content/uploads/2016/06/internet-dataandtrade-meltzer.pdf.
- For instance, some countries, such as Malaysia, permit transfers only with the explicit consent of the data subject. In some cases, this can serve as a significant impediment.
- Anupam Chander, Uyên P. Lê, Data Nationalism, 64 Emory L.J. 677 (2015),http://law.emory.edu/elj/content/volume-64/issue-3/articles/data-nationalism.html;
- D. Castro, The False Promise of Data Nationalism, December 2013, http://www2.itif.org/2013-false-promise-data-nationalism.
- C. Kuner, Data Nationalism And Its Discontents, Emory Law Journal, 2015 https://brusselsprivacyhub.eu/onewebmedia/kuner.
- Zachary D. Clopton, Territoriality, Technology, and National Security, 83 U. CHI.L.REV. 45 (2016)
- A.Woods, Against Data Exceptionalism, Stanford Law Review, 2016
- https://uknowledge.uky.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1593&context=law_facpub
- C. Kuner, Data Nationalism and Its Discontents, Emory Law Journal, 2015. https://brusselsprivacyhub.eu/onewebmedia/kuner.pdf
- M.F. Ferracane, E. Marel, The Cost of Data Protectionism, October 2018. http://ecipe.org/blog/the-cost-of-data-protectionism/
- C. Chelliah, With Data Sovereignty, Location Isn't Everything. https://www.oracle.com/uk/cloud/paas/features/data-sovereignty/
- J Labour, Data sovereignty: What you need to know and why you should care, 24 January 2018. https://cira.ca/blog/state-internet/data-sovereignty-what-you-need-know-and-why-you-should-care
- Couldry, Nick and Mejias, Ulises (2018) Data colonialism: rethinking big data's relation to the contemporary subject. Television and New Media. ISSN 1527-4764
- Simon Kemp, The Full Guide to Southeast Asia's Digital Landscape, TechinAsia, Feb. 8, 2017, www.techinasia.com/talk/full-guide-southeast-asia-digital-landscape-2017 Han-wei liu, Data Localization and Digital Trade Barriers:ASEAN in Megaregionalism, 371-391, (2018. https://www.researchgate.net/publication/332059133Christopher Kuner, Transborder Data Flows and Data Protection Law 26–7 (2013); Allan Gotlieb et al., The Transborder Transfer of Information by

Communications and Computer Systems: Issues and Approached to Guiding Principles, 68 Am. J. Int'l L. 227, 246 (1974).

- Scott Shane, Ex-Contractor Is Charged in Leaks on N.S.A. Surveillance, N.Y. Times,June 21, 2013, www.nytimes.com/2013/06/22/us/snowden-espionage-act.html? mcubz=1
- Jonah Force Hill, The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders, Lawfare Research Paper
- Series 3 (2014), https://lawfare.s3-us-west-2.amazonaws.com/staging/Lawfare-ResearchPaper-Series-Vol2 No3.
- Anupam Chander & Uyên P. Lê, Data Nationalism, 64 Emory L. J 677 (2015).
- Shin-Yi Peng& Han-Wei Liu, The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?, 51 J. World Trade 183, 190 (2017).
- Graham Greenleaf & Scott Livingston, China's New Cybersecurity Law – Also a Data Privacy Law?, 144 Privacy Laws & Bus. Int'l Rep. 1-7 (2017).
- Ryan M. Calo, Against Notice Skepticism in Privacy (and Elsewhere), 87(3) Notre Dame Law Review (2012) at p. 1049
- Sanjay Kishan Kaul, J., in Puttaswamy, (2017). referring to the Second Circuit's decision in Haelan Laboratories v. Topps Chewing Gum. 202 F.2d 866 (2d Cir. 1953) Adam Moore, Toward Informational Privacy Rights, 44 San Diego Law Review (2007) at p. 812; Anita L.Allen, Why privacy isn't everything: Feminist reflections on personal accountability (Rowman & Littlefield, 2003) at pp. 115-16; John Kleinig, The Nature of Consent in The Ethics of Consent- Theory and Practice (Alan
- Wertheimer and Franklin Miller (eds.), Oxford University Press, 2009) at p. 4.
- Ryan M. Calo, Against Notice Skepticism in Privacy (and Elsewhere), 87(3) Notre Dame Law Review (2012) at p.1031.
- Reidenberg et al, Privacy Harms and the effectiveness of the Notice and Choice Framework, 11(2) Journal of Law and Policy for the Information Society (2015)
- Florian Schaub et al, A design space for effective Privacy Notices (Symposium on usable privacy and security, 2015) at p. 2; LF Cranor, Necessary but not sufficient: Standardized mechanisms for privacy notice and choice, 10 Journal on Telecommunications and High Technology Law (2012) at p. 273.
- B. W. Schermer et al, The crisis of consent: how stronger legal protection may lead to weaker consent in data protection, 16(2) Ethics and Information Technology (2014).