

RECOMMENDATIONS
ON

DRAFT

PERSONAL DATA
PROTECTION BILL
2018

**CYBER SECURITY RESEARCH CENTRE
&
CYBER PEACE FOUNDATION**

PROCEEDINGS OF WORKSHOP CONDUCTED ON
DRAFT DATA PROTECTION BILL (2018)

Foreword

The Information Age as we have seen is a positive outcome of Technology. However, it comes with its own national security challenges. As with all ages right from the Stone Age, Bronze Age etc in human history, nations and societies that adapt and recognize these challenges and opportunities prevail while others decline. While many see these opportunities in a positive manner and use it accordingly, others seize the openings for negative purposes.

The 21st century and the information revolution bring about rapid and disruptive changes at a pace that have never been witnessed in human history. In this context the Supreme Court of India recognizing Privacy as a fundamental right of citizens in the 'Puttaswamy vs Union of India' is historical with profound implications for India. The data protection whitepaper by the Justice Srikrishna committee is a logical step by the government and will eventually lead to a Privacy Law.

The Cyber Security Research Centre (CSRC); Punjab Engineering College (PEC) organizing this workshop to review this White Paper from a national security viewpoint is a welcome and extremely important initiative. With India rushing into the Information Age with projects like Digital India, 100 smart cities and Aadhar. There is an urgent need for a legal framework to address the billions of sensors filled with personal data, a large-scale surveillance network that will exist without constitutional safeguards. Redefining effects to protect this data is a necessary step toward providing a measure of protection. The Privacy law is needed not only to safeguard the privacy of the citizens but also to safeguard the very security of the nation. The military implications of a national level surveillance grid controlled by MNC's and being able to access data from an exponentially growing grid is a challenge which India has to address. The workshop is a comprehensive review of those challenges and brings out the great economic opportunity that exists for India in addressing those challenges. A very useful compendium wherein some of the best strategic brains of the nation has worked on and should guide India in various policy initiatives for the 21st century. A must read for all academics, military scholars and members of Parliament who will participate in the enactment of the Privacy Law.



(SHEKHAR DUTT)

CONTRIBUTORS

1. Sh. Satyendra Pradhan, Former Dy. NSA and JIC Chairman, Member, Advisory Board, CSRC
2. Lt. Gen. D.S. Hooda , Former GOC-in-C, Member, Advisory Board, CSRC
3. Mr. S.N. Pradhan, IPS, Joint Secretary, Ministry of Development of North East
4. Dr. Divya Bansal, Prof. & Head, Cyber Security Research Centre, *PEC*, Chandigarh
5. Dr. Sanjeev Sofat, Prof. & Head, CSE
6. Sh. Pavithran Rajan, Adjunct Faculty, CSRC
7. Col N.P. Singh, Perspective Planning Directorate
8. Dr. Upasna Saluja, Senior Cyber Security Consultant, AT&T Cyber Security Consulting
9. Mr. Vineet Kumar, CPF Policy Team
10. Ms. Geeta Gulati, Advocate
11. Mr. Dinesh Bareja, COO Open Security Alliance
12. Dr. Manvjeet Kaur, Asst. Prof., CSRC
13. Ms. Sawinder Kaur, Asst. Prof., CSRC
14. Ms. Amrita, Director Advisor, Cyber Cafe Association of India (CCAOI)
15. Mr. Nitish, CPF Policy Team
16. Mr. Raj, CPF Policy Team
17. Mr. Abhay, CPF Policy Team
18. Ms. Chesta Sofat, Research Scholar, CSRC
19. Ms. Megha, Research Scholar, CSRC
20. Ms. Jaspal Kaur Saini, Research Scholar, CSRC
21. Ms. Rashmi, Research Scholar, CSRC
22. Mr. Sidhant, Research Scholar, CSRC
23. Ms. Japneet, Research Scholar, CSRC
24. Mr. Sanjay Madan, CDAC, Mohali and Research Scholar, CSRC
25. Mr. Shisrut Rawat

Background

Privacy and Data Protection is a subject that has seen massive developments in the last few years. Undoubtedly, with the advent of social media, big data and blurring jurisdictions and processes, there have been many questions about data and its rationale in national security, rights of citizens, generator of wealth etc.

The **Cyber Security Research Centre (CSRC)** at Punjab Engineering College (Deemed to be University); Chandigarh had organised a previous workshop to carry out a study of the Justice Srikrishna Committee White Paper on Data Protection, examining it from a National Security Perspective on Jan 28, 2018. The findings of the study were presented in the form of a report carrying recommendations to Meity; GoI which were duly considered. This report was also widely appreciated as this was the first of the studies to explore the dimensions of privacy from a national security perspective.

Cyber Peace Foundation (CPF) and Policy Perspectives Foundation (PPF) thereafter held the second edition of their joint round table conference, Securing Cyber Space, on the 7th of September 2018. The theme for this year's conference being Data Protection. In the multiple sessions, there were recurring questions pertaining to the draft Personal Data Protection Bill released for comments and India's recent dive into the Right to Privacy and Data Protection space.

There have been multiple citizen movements centric to the idea of data privacy and rights of data principals/users. Debates about surveillance, data localisation, defining key terms and the concurrence with the GDPR have been ongoing and have slowly occupied centre stage. As a result of these discussions with various experts and recent developments in the domain, it was felt that a comprehensive list of comments and recommendations must be prepared after brainstorming exercises with multiple stakeholders. Data, in the long run is most likely going to drive nations, policies and international relations as well. To further this objective of understanding the draft bill and working on the issues that it has presented, there is a need to present the challenges to national security and the economic opportunities of the privacy debate to the lawmakers.

It is widely accepted that there can be no privacy without security. The Cambridge Analytica scandal and the dangers of Information Warfare was clearly highlighted post the first workshop conducted at CSRC, PEC wherein our recommendations towards the need for data localisation at that time considered too stringent was vindicated.

The second workshop post Cambridge Analytica found widespread unanimity among multiple stake holders on the need for stringent provisions to protect the privacy of citizens and also guard national security. The members also understood that in a liberal, open society like ours there needs to be different laws/provisions to cover CII (Critical Info

Infrastructure) where the Government and various sensitive organizations and their manpower are covered with special provisions. The members consensually agreed that Indigenous Technology will be a key component in this particular data protection framework for to attain national security.

In context of data localisation, it is pertinent to note Russia's case study of the adoption of a nationwide policy and effective implementation as well. Many companies, even the giants like booking.com, Apple etc. moved their server spaces within Russian boundaries owing to the legal provision for data localisation. They made use of a local vendor's services for storing data in Russia, which definitely fueled the thought and discussion on how Russia has supported its private industry as well as dealt with an ailing economy. Data centres in Russia grew over 20% year on year and as of date, the supply exceeds the demand. Along the same lines now, major companies like Facebook and Google are also being offered server space by domestic vendors, these have given the data analytics market a fillip adding to employment generation and economic benefit of the country.

The need for technologies not controlled by other nations in CII has been felt in states like Germany too. The availability and controllability of security technology – in terms of technological sovereignty – will be in the future for Germany's security policy in both the civilian and military sectors. There is broad agreement nonetheless that not only armed forces but also businesses and citizens need to have the latest security technology in order to fulfil their responsibilities, protect themselves and to protect infrastructure, in particular critical infrastructure. The importance of having national "core capabilities" and "key security technology," particularly in the defence sector and for secure IT systems, it has not yet clearly defined these terms. The potential relevance of many important fields of technology for our national security has not yet been considered. This include new materials and production processes such as 3D printing, sensor technology, robotics and miniaturisation, energy storage technology, biotechnology, and navigation and geodata systems as the basis for any kind of automated motion. The importance of these technologies is currently only discussed, if at all, in their economic or scientific context. There are no transparent criteria to classify "key technologies" nor are there any clearly articulated objectives on how these will be integrated into industrial policy and what the consequences will then be for the businesses in these sectors.

Digitized information, is being processed automatically to draw inferences that have economical impact. An example of how exhaustive and expansive the detailed digitised information of people's activities and behaviour that is being collected can be better understood by a comparison between digital data the NSA stores, with the amounts of files the Stasi – German Democratic Republic's domestic secret service – produced. It is

estimated that entire information captured throughout the Stasi history; considered a feared arm of totalitarian state is estimated to fill about:

- A) 48.000 cabinets
- B) Covering approximately 0,019 km²

The NSA's data centre in Utah will host about:

- A) 5 zettabytes of data
- B) Roughly 42 quadrillion file cabinets covering 17 million km² (If converted into hard copy)

This is an area bigger than the European continent. The example above also shows the differing efforts needed to collect and archive data depending on whether using analog or digital data processing. While the Stasi needed to install microphones, hire staff to monitor and document people's behaviour to gain information about their habits, attitudes and social networks, in a digitized world a lot of that information can be monitored and stored on the fly through sensors, log data or user generated content. This heterogeneous form of digitised data can be used to extract knowledge and profile each individuals and this data becomes easily exchangeable worldwide for further processing, storage or analysing.

Thus from the above example it is quite evident that proposed data protection legislation has huge economic repercussions on big data aggregators, primarily MNCs based in the US. These companies have reacted with alarm to the planned legislation and has openly declared their intentions to lobby for continuation of status quo. The participants of the workshop took note of these developments and accepted that a large part of the literature on privacy and the debates on privacy post the Puttaswamy Judgement has been curated by these giant MNCs. The workshop has paid special attention to bring out the economic benefits that will accrue to the nation by data localisation and have now given their recommendations for more stringent provisions beyond what was recommended in the first workshop. It is hoped that this document will help the MEITY officials and the law makers and present an unbiased view point. For those who might think that the law that emanates from this document might be more stringent than other initiatives by other nations, it is submitted that our law is being planned post Cambridge Analytica and wherein the nature of warfare and the dangers to our social fabric in the Information Age is much more clearer.

RECOMMENDATIONS

Recommendation 1: Privacy must be incorporated right from the time an individual takes birth. The culture of privacy should be included in the educational system at all levels. The prominent stakeholders such as the government, central and state boards, along with civil societies should take joint initiatives for the same. As for on the ground implementation, the data protection awareness fund shall be utilized for awareness initiatives and curriculum development for privacy education at the basic levels and to build short books, reference material, educational videos etc.

Recommendation 2: Under Section 50 of the bill which discusses composition, qualification of members to the Data Protection Authority, clause (4) shall include “a person having professional or specialized knowledge in the subject matters including to but not limited to –

- a) National Security
- b) Law Enforcement
- c) Financial/Insurance
- d) Technology and Law

Inclusions of experts from multi-disciplinary backgrounds is necessary as the functions of these domain relies heavily on the internet and related technologies.

Recommendation 3: For powers of DPA given under Section 62-66, the persons authorized by the authority must have techno legal background to ensure that the maximum level of efficiency and legal compliance is achieved.

Recommendation 4: The Personal Data Protection Act (Singapore) defines personal data under Section 2 as “data, whether true or not, about an individual, who can be identified from the data, or from that data and other information through which the organization has or likely to have access”. By bringing in the principle of identity, this act has curbed the need for distinguishing between various types of personal data of the data principal. [3]

The idea that we are proposing is to completely exclude terms like anonymization, pseudo-anonymization from the purview of this bill. Hence, the provision excluding the anonymized data from the scope of this bill i.e. Sec 2(3) must be necessarily removed. Personal data should be actually only viewed as personal data with no fetters. If there is some data that can actually be anonymized in the true sense and no activity can lead to identification, we feel it doesn't affect any purpose. At the same time, we must also bear in mind that any future development in this field may lead to identification and correlation of data leaving the data principal exposed. A proactive and balanced approach is to have just define personal data and not go into the depths of excluding any diluted version of it.

Recommendation 5: The definition given under Sec 2(21) does not cover instances of psychological harm to data principal due to processing of either his personal data or sensitive personal data. Further, the report published along with this bill also talks about online radicalization.

In addition, the harm that might be caused is only covered u/s 32 (Personal Data Breach). Any other instances due to processing of an individual's personal data gives rise to a conflicting situation in the existing legal regime. One of the possible foreseeable conflicts can be applicability of this bill or the Information Technology Act.

In an ordinary setting, we recommend that due to the processing or profiling activities, if any data principal is made to face psychological harm like political or anti-national motivation or advertisements, it should be penalized.

Recommendation 6: The bill has defined personal data u/s 2(29) and sensitive personal data u/s 2(35). We suggest that an additional category can be created in parallel with the present classification [12]. It can be termed as "Sensitive Personnel/Organization". This category shall include defense personnel, Judges presiding over the courts having constitutional power, statutory bodies dealing with CII (Critical Information Infrastructure) among the others.

The idea behind this classification is to give them additional layer of rights and protection while they are discharging their official duty. If the final realization is that having them under critical data is sufficient, that is also acceptable but the fact that there need to be some establishments and personnel with higher degree of protection, remains.

Recommendation 7: Amendments to the Aadhaar Act:

- a) Majority of the discussion of data privacy and protection revolves around Aadhaar and the UIDAI Act. However, this bill is completely silent on its retrospective effect on a government database as large as the Aadhaar. Aadhaar must be brought under the scope of this act. (Sec 91)
- b) The report suggests a wide range of amendments to the Aadhaar Act which includes giving significant amount of power for enforcement, imposing penalties etc. In our view, the role of UIDAI shall be kept limited to a data fiduciary. Otherwise, in disputes related to a data principal's Aadhaar data, there will be clear cut conflict of interest for UIDAI to hear a matter against their own processes and functions.

Hence it is recommended to bring UIDAI as well as its operations and functions under the scope of this bill so that they can be questioned on reasonable grounds [5].

Recommendation 8: Section 40(1) mandates every data fiduciary to store at least one serving copy of personal data within a server or data center located in India.

We strongly oppose the concept of having mirror copy as it is completely averse to the principle of Data Privacy. Not just that, a serving copy of the data still poses the same levels of threats to the data. As for the impact of a stringent data localization requirement, this report goes on to discuss the issue separately. The personal data of Indian data principals must reside within the territory not just to ensure security and privacy but its quality as well [16 – 17, 19].

Recommendation 9: Section 41 deals with conditions for cross border transfer of personal data. The grounds given in clause 1 shall also include model contracts with other nation states. It should also be cleared whether cross-border data flow would be termed as processing under the definition of the Act leading to a situation where non-consensual cross border data flow might also be undertaken [6].

The GDPR allows for the flow of data to third party countries if the receiving country's laws are in compliance with the GDPR's rules. This is where friction lies between the approaches followed by U.S. and EU [20]. While the GDPR guidelines pertain to EU member states, many EU members have their own nation-specific data laws which heighten complexity, confusion and cost. For example, the Danish Bookkeeping Act requires firms to store financial data of Danish citizens in either Denmark or another Nordic country for five years. Greece enacted a data localization law in 2001, stipulating that data generated on physical media located in Greece must be stored on Greek territory. Germany established its own data localization laws, with slight deviations from the GDPR. If data is meant for further processing, it does not have to come under the same regulations designated by the GDPR if those regulations would disproportionately affect the further processing of the data. Germany also requires any company with at least ten employees to have a data protection officer, although the GDPR only stipulates the need for one in exceptional circumstances.

Recommendation 10: Notice u/s 8 –

- a) Digital literacy in India is not at par with developed countries hence u/s 8(2) shall also include a situation where the citizen is illiterate and unable to understand the written material and its implications.
- b) A color-coded scheme can be implemented to signify the level of severity involved in processing of data. (like highlighting sensitive personal data attributes red and so on)
- c) The purpose of data collection whether the data is manually processed or is processed automatically should be mentioned in notice [8].
- d) In case the data so collected is profiled, the same has to be notified in the form of a separate consent. Clause 1 of Sec 8 must state it clearly [8].

Even if the understanding of the meaning of automated profiling varies among countries, the DPAs of EU agree in three principal characteristics of profiling:

1. It is based on a collection, storage and/or analysis of different kind of data;
2. and on automated processing using electronic means;
3. with an objective of prediction or analysis of personal aspects or personality and/or the creation of profile.

Profiling is defined as “any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person’s performance at work, economic situation, location, health, personal preferences, reliability, or behaviour”. Additionally, a fourth key aspect for some DPAs is that the profiling results in legal consequences for the data subject. There is need of a legal definition of profiling in order to clarify the definition and conditions it can be used. Three DPAs (Hungarian, Swedish and British) are not in favour of a definition by law because it would create misinterpretation and it would be difficult to provide an exhaustive definition including every imaginable profiling situation. Also, on-line tracking tools, the Regulation explicitly mentions that “cookie identifiers” as well as RFID tags [10][13][14].

Recommendation 11: Since the motive of Chapter V of the bill is to give maximum level of protection to children, we suggest that:

- a) Significant data fiduciaries must not be allowed to be suo-moto existent. They should undergo a process of scrutiny and structured vetting before being allowed to collect or process data of children to whatever permissible limit as well.
- b) The authority can either invite public comments for approving a guardian data fiduciary or at least have a process of objection because there are known organizations and people dealing in children’s’ data.

Recommendation 12: There needs to be a mechanism to verify the age of the children while using different online services so as to restrict them to services that require the user to be an adult.

We suggest that a virtual ID can be generated from their respective Aadhaar numbers. The virtual id only contains the details about the age of an individual. This virtual id can be used to access services only if a person is above the specified age for different services. In this way no personal data is being shared with any data fiduciary and only the age is being shared using virtual id, which cannot be tracked back to the original Aadhaar Data. [4]

Recommendation 13: The power given u/s 60 & 61 of the bill for prescribing technical standards and prescribing codes of conduct presently resides with the DPA.

We suggest that a different board such as the Banking Codes and Standards Board of India (BCSBI) empaneling multi-disciplinary experts must be given the power to decide over the standard technical standards that need to be used by the data fiduciary. We also recommend developing Indian Security Standards for handling and managing CII.

Recommendation 14: Rights under Chapter VI –

- a) Right to be forgotten given u/s 27 has a limited scope and enforcing this right doesn't result in deletion of data, it only restricts or prevents disclosure of the data for the purpose of processing. [11] The scope of this right must be widened to include the right to erasure. It should cater to following scenarios:
 - a. When a Legal Deadline Expires
 - b. When the Conditions of Lawful Data Processing Are Not Met
 - c. At Pre-defined (or Default) Dates
 - d. Grey Zone: Data of the Deceased
- b) The general procedure given u/s 28 for exercising of right given under chapter VI specifies making a request to the data fiduciary for exercising a particular right. However, right to be forgotten u/s 27 specifies making an application to the Adjudicating Officer (AO). Even for the enforcement of this right a reasonable time needs to be given to the data fiduciary for erasure/deletion/removal of personal data of a data principal in order uphold the principles of natural justice. In practical application, it will be tedious task for the data principal to attend hearings at the AOs office after initiating quasi-judicial proceeding without giving them reasonable opportunity for erasure/deletion/removal of the data.
- c) Though withdrawal of consent is mentioned in Sec 8(1)(d) and 12(2)(e) it must be recognized as a separate right under this chapter so that it can be enforced as per the conditions given u/s 28 [11].

Recommendation 15: Processing for grounds other than consent. (Sec 13-17)

- a) Apart from these grounds, second schedule PDPA Singapore also includes legal services, sharing of personal data of citizens between public agencies for purpose of policy formation etc. These may also be incorporated.
- b) The extent of reasonable purposes given under sub clauses (d) and (g) of Section 17(2) must be restricted.
- c) In Sec 15(c), the phrase “any breakdown of public order” needs elaboration or restriction like the possibility of clear and imminent danger.
- d) Alternatively, it should be mandated through this Act that when anyone in exercise of his powers by virtue of the non-consensual processing does any action with respect to someone's personal data, they must note the reasons in writing of such actions. We propose that for every decision taken u/s 15,

the decision making person must record his reasons in writing for processing the personal data of data principal without his consent.

Recommendation 16: Chapter IX Exemptions –

Apart from the exemptions given under this chapter, we also propose inclusion of following-

- a) Armed Forces
- b) Parliamentary/Judicial Privileges
- c) Professional Privileges (Doctors and Advocates)
- d) Mark-sheets and transcripts

Recommendation 17:

Consent is to be considered multi-dimensional. It should not be taken as one-time permission to collect personal information. Lacking the opportunity to provide informed consent, the individual is effectively disempowered. The consent should also be exercised in different forms including:

- a) Consent Obtained by Browser Settings
- b) Consent Given by Opt-out Mechanisms
- c) Prior Opt-in Consent

PDP should be consistent with the market practice that is now being shaped around the implementation of cookies' consent, requesting an affirmative action of the on-line user (be it through clicking on an "I accept" or "ok" box on a website banner or by use of another technique) before installing the tracking application. In consequence, pre-configuration of the browser settings so that cookies are installed unless the individual opts out do not appear to be in-line with the "affirmative" action to the notion of "consent" [14].

Recommendation 18: Chapter III, Clause 16 specifies: Processing of personal data necessary for purposes related to employment.

The members observe that employees as data subjects often are double victims once as citizens and consumers and secondly as dependent workers. Personnel administration by personal information systems, personal data created by the use of email and the internet, data of working time records, attendance and sickness records, data from video cameras, and many more information and communication technologies (ICT) are implemented on company levels generating and administrating personnel data. The DPDP should not distinguish between consents given to be sought by an employee as a data subject under any circumstances [15].

Does Data Protection & Privacy not stand in the way of Innovation?

The new issues posed by technological development challenge current and future regulation to adequately respond to matters related to self-determination especially regarding the problem of the general applicability of data protection to profiling and the efficiency of technical approaches such as anonymity and de-identification. It is paramount to enhance the critical thinking on the possibilities, as well as the limitations, of improving data protection in the current and future technological setting.

Some debates around have been trying to suggest that rigid adherence to general privacy principles inhibits innovation and interferences with economic and social progress, and that these limits should be relaxed. We should be wary of good intentions and seek ways to achieve positive-sum outcomes. Many of the perceived barriers associated with obtaining informed consent, specifying and limiting purposes, and restricting collection and uses of personal information can be obviated by applying innovative methods and widely available data processing techniques. Many Big Data applications may be achieved using de-identified data in place of identifiable personal information. The European Data Protection Commissioners have developed criteria and practical guidelines on open data and public-sector information re-use, as has the Office of the Information and Privacy Commissioner of Ontario, Canada [18].

Privacy and data protection are at times contrasted with other legitimate societal values and goals, with the suggestion that one area must yield to the other. It is not necessary to weaken existing privacy measures in the name of pursuing greater efficiencies, innovation and economic growth. Further, there is a long and growing list of public and private-sector authorities in the United States, the EU, and elsewhere, who unequivocally endorse a proactive approach to privacy as a more robust application of FIPPs, and as a critical means by which to establish sufficient, necessary trust in the evolving information economy.

Privacy by Design Foundational Principles build upon universal FIPPs in a way that updates and adapts them to modern information management needs and requirements. By emphasizing proactive leadership and goal-setting, systematic and verifiable implementation methods, and demonstrable positive-sum results, Privacy by Design principles can assure effective organizational privacy and security by:

- serving as a framework for domain-specific control objectives and best practices;
- reducing harms and other “unintended” consequences associated with personal information;
- strengthening internal accountability mechanisms;
- demonstrating effectiveness and credibility of data management practices;
- supporting regulatory and third party oversight efforts;
- earning the confidence and trust of clients, partners and the public; and

- promoting market-based innovation, creativity and competitiveness.

There is a growing understanding that innovation and competitiveness must be approached from a “design-thinking” perspective – namely, viewing the world to overcome constraints in a way that is holistic, interdisciplinary, integrative, creative and innovative. The future of privacy must also be approached from the same design-thinking perspective. Privacy and data protection should be incorporated into networked data systems and technologies by default, and become integral to organizational priorities, project objectives, design processes, and planning operations. Ideally, privacy and data protection should be embedded into every standard, protocol, and data practice that touches our lives. This will require skilled privacy engineers, computer scientists, software designers and common methodologies that are now being developed, hopefully to usher in an era of Big Privacy.

Bibliography

- [1] Carnegie-Mellon University CyLab Usable Privacy and Security Laboratory (CUPS), <http://cups.cs.cmu.edu>.
- [2] “Exploring Privacy – A Roundtable Series,” <http://www.ftc.gov/bcp/workshops/privacysoundtables/index.shtml>.
- [3] “Future of Identity in the Information Society (FIDIS),” www.fidis.net.
- [4] “IPSI Smart Data International Symposium,” <http://www.ipsi.utoronto.ca/sdis/>.
- [5] “Personal Data Ecosystem Consortium,” <http://pde.cc/startup-circle>.
- [6] “Privacy and Identity Management for Community Services (PICOS),” www.picos-project.eu.
- [7] “Privacy and Identity Management for Europe (PRIME),” www.prime-project.eu.
- [8] “OECD Privacy Principles,” <http://oecdprivacy.org>.
- [9] “Trustworthy Clouds Privacy and Resilience for Internet-Scale Critical Infrastructure (TClouds),” www.tclouds-project.eu.
- [10] Ann Cavoukian, “Identity Theft Revisited: Security Is Not Enough”, Office of the Information & Privacy Commissioner of Ontario <http://www.ipc.on.ca/images/Resources/idtheft-revisit.pdf>.
- [11] Ann Cavoukian, “Personal Data Ecosystem (PDE) – A Privacy by Design Approach to an Individual’s Pursuit of Radical Control,” in Digital Enlightenment Forum Yearbook 2013: The Value of Personal Data. M. Hildebrandt, K. O’Hara and M. Waidner (eds). IOS Press, 2013.
- [12] Ann Cavoukian, “Privacy by Design: Leadership, Methods, and Results,” in European Data Protection: Coming of Age, ed. S. Gutwirth et al. (New York: Springer, 2013), 175.
- [13] Ann Cavoukian, Privacy in the Clouds: Privacy and Digital Identity – Implications for the Internet 2008 <http://www.ipc.on.ca/images/Resources/privacyintheclouds.pdf>.
- [14] Ann Cavoukian, Privacy by Design: The 7 Foundational Principles. Office of the Information & Privacy Commissioner of Ontario, 2009.
- [15] Framework to Ensure That Privacy Risks Are Managed, by Default”, Office of the Information & Privacy Commissioner of Ontario <http://www.privacybydesign.ca/publications/accountable-business-practices>.
- [16] https://jsis.washington.edu/news/russian-data-localization-enriching-security-economy/#_ftn22
- [17] http://www.ecipe.org/app/uploads/2014/12/ECIPE_bulletin914_dataoloc_indonesia.pdf
- [18] http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf - this paper has simulations of GDP and localisation scenarios.
- [19] https://www.alexandria.unisg.ch/247544/8/Mihaylova_Data_localisation_2016.pdf
- [20] <https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/data-localization-free-all>

Recommendations on White paper on Personal Data Protection (2017)



Workshop Proceedings on
Study of the Justice Srikrishna Panel Paper

Data Protection

FROM A NATIONAL SECURITY PERSPECTIVE

January 29 - 30, 2018

CYBER SECURITY RESEARCH CENTRE

Punjab Engineering College, Chandigarh

ACKNOWLEDGEMENTS

1. Dr S.D. Pradhan - Former Dy NSA and JIC Chairman
2. Sh. P.C. Haldar - Former DIB and NSAB Member
3. Lt. Gen. DS Hooda - Former Army Commander
4. Dr. N. S. Kalsi, IAS,
Additional Chief Secy- Development, Punjab
5. Dr. Divya Bansal, Head, CSRC, PEC ([Point of Contact](#))
6. Sh. Pavithran Rajan, Adjunct Faculty, CSRC
7. Dr. Manvjeet Kaur, Asst. Professor, CSRC, PEC
8. Sh. Naunihal Singh, IPS. IGP/Cyber Crime
9. Adv. Geeta Gulati, Punjab & Haryana High Court
10. Mr. Vineet Kumar, President, Cyber Peace Foundation
11. Mr. Purnendu Singh,
Director Operations, Cyber Peace Foundation
12. Mr. Nitish Chandan,
Policy and Advocacy Team, Cyber Peace Foundation
13. Ms. Chesta Sofat, Research Scholar, CSRC, PEC
14. Ms. Tanvi, Research Scholar, CSRC, PEC
15. Ms. Jaspal Saini, Research Scholar, CSRC, PEC
16. Ms. Saawinder, Faculty, CSRC, PEC
17. Mr. Mohit Jain, Infosys, Chandigarh

INTRODUCTION

As India moves towards a digital future, the importance of personal data of its citizens is becoming crucial to protect national interests. Much of the debate on this subject is centred around an individual's right to privacy. As the Supreme Court observed in *Puttaswamy*, *“Informational Privacy is a facet of right to privacy. The dangers to privacy in an age of information can originate not only from the state but non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state.”*

In order to formulate a data protection law, the Government of India has drafted a white paper, which outlines some important issues, which require incorporation in the law. The White Paper has sought public comments on the shape of the data protection law.

The White Paper is an extremely comprehensive compilation, which not only brings out the key facets of data protection but also studies provisions from laws of other countries to evaluate best practices.

Most of the analysis in the White Paper has looked at data protection from the prism of protecting an individual's right to privacy, while ensuring that it does not become so overpowering that it hinders freedom of expression, research, artistic rights, law and order requirements etc. However, if there is one area that the White Paper has not focused on, it is in on the national security implications of personal data.

In the current digital era, and the forthcoming explosion in the Internet of Things and Big Data Analytics, each individual is generating a vast amount of data. Taken individually, this data may seem unimportant, but when aggregated and analysed

through advanced algorithms, it can reveal crucial information, which have important national security implications.

A recent example is the details released by Strava, a fitness-tracking app, showing activity of its users on data visualisation map. The map was detailed enough to show the activity of U.S. soldiers in their bases including Afghanistan, Syria and Djibouti. This revealed sensitive information about the layout of bases. Firms like AggregateIQ and Cambridge Analytica have been credited with using personal data of individuals to generate targeted advertisements on social media to help swing the Brexit referendum and the US presidential election. There are many consequences to personal data collection, which we have not fully grasped till now.

In order to bring in the national security perspective into our proposed data protection law, the Cyber Security Research Centre of the Punjab Engineering College, Chandigarh in collaboration with the Times of India, organised a two day workshop which brought together experts from the national security, cyber security, academicians, information technology, military, law enforcement and legal fields.

The deliberations of the workshop and its recommendations are being put forth for consideration by the Government of India. There was unanimity among the members of the workshop that national security implications be given due consideration while drafting the data law. Absence of any legal provisions about protection of individual data has already resulted in sensitive data of Indians having possibly been utilised and processed in an unregulated manner. There is uncertainty about what national security problems it could create in the future but let us now begin the corrective steps.

Summary

The deliberations of the workshop have raised many crucial issues with regard to the linkages between unfettered processing of individual data and matters of national security. We have kept in mind the individual's right to privacy, particularly the vulnerabilities of children and underprivileged class. Due consideration has also been given to digital commerce and the need to ensure that innovation and entrepreneurship in India is not disadvantaged. However, we are also conscious that economics cannot override national security. As John J. Mearsheimer points out in his book, *The Tragedy of Great Power Politics*, "(In) matters of national security, because concerns about survival are invariably at stake...they are more important than worries about prosperity."

Some key recommendations are summarised below.

Data Localisation

Our discussions revealed the territorial limits of jurisdiction. It is extremely difficult to protect data which resides in other countries, particularly where the data controller does not have any presence in India. U.S. courts are even asking technology companies registered in the country to provide data, which is located outside the U.S. borders. One way suggested was to have bilateral treaties with various countries but this a protracted process.

The only solution lies in localising the sensitive data of Indian citizens within the boundaries of India. While currently the infrastructure for this may not exist, it would come up if the data controllers wish to continue to take advantage of the size of the Indian market.

The advent of the IoT would exponentially increase the volume of data being generated. Any new infrastructure being created for IoT should also make arrangement for data to be stored in India.

We understand that cross-border flows of data cannot be completely stopped. However, no sensitive personal data should be permitted to go outside the country. There should be legal restrictions on transfer of data to controllers who have no presence in India.

Sensitive Data

The White Paper has given a comprehensive definition of sensitive personal data. However, this definition is based on the sensitivity of the information from an individual perspective and not from national security. As an example, should the data of intelligence officials or military officers, stored in one place, be considered sensitive, even though it has only basic personal data? There could be many such cases and therefore there is a need to classify such data also as sensitive. Also, in the new connected world where IoT devices are penetrating into the personal lives, the sensory raw data does not indicate anything but it is the processed data leading to sensitive inferences so drawn about an individual which will pose a greater risk.

Data Processing

Individuals are generating data vast amount of data each time they carry out any electronic activity. This information is automatically stored by data controllers. It is difficult to keep a check on this activity but the processing of data must be for a specific and limited purpose.

With aggregation of data and advanced algorithms for processing, it is possible to build up an accurate profile of an individual which reveals many traits of his character. This knowledge could be used to influence opinions or even stir up trouble

and strife between communities. Such analytical profiling can be checked if the processing of data is strictly controlled. Sale of personal data to data brokers must also meet stringent legal criteria.

Individual Rights

By having greater control and visibility over their data, individual can indirectly contribute towards national security. The white Paper has correctly identified Individual Participation Rights like confirmation, access to data, right to object and the right to be forgotten. These will strengthen individual privacy.

In addition to these it is important that an individual is aware of all the data controllers who have access to his personal data. This is important because data is regularly being shared between various entities without the individual coming to know. This will also put some check on the practice of routinely asking for personal data even when not essential.

Economic Impact

A reading of the White Paper shows that there is some apprehension that a stringent data law could have an adverse financial impact. In our discussions, we did not find any fact that could support this apprehension. In fact, in the long term, data localisation and development of Indian Standards will help the indigenous industry.

Foreign Investment firms will need to set up their data centres within the territory of India and this will mean newer opportunities for the Indian IT skilled professionals. The government will be motivated to setup an in-house IT industry and start-up sector focusing on development of Indigenous technology. With Data Localisation a lot of personal data of the Indian Residents will return to Indian borders. There will be a large scope for domestic data transformation projects. Many MNCs will be compelled to start with migration projects which in turn will fetch a lot of capital.

Conclusion

The need for a data protection law was triggered by the debate on individual privacy. However, the importance of this data for national security must not be overlooked. It is for this purpose that the workshop held at PEC focused on the how the proposed law must also strengthen India's national security.

SCOPE AND EXEMPTIONS

Chapter 1. Territorial and Personal Scope

The power of the State to prescribe and enforce laws is governed by the rules of jurisdiction in international law. Data protection laws challenge this traditional conception since a single act of processing could very easily occur across jurisdictions. In this context, it is necessary to determine the applicability of the proposed data protection law.

Questions

1. What are your views on what the territorial scope and the extra-territorial application of a data protection law in India?

Ans. The definition of extra territorial entity should be clear.

The law of the land should be followed which implies a person residing within Indian borders will be covered under the Indian data privacy act.

As per Provisional views, The Privacy Act should be applicable to :

- Processing of personal information which takes place in the territory of India by entities which have a presence in India.
- Entities which may not have a physical presence in India but carries on a business or offers goods or services in India

2. To what extent should the law be applicable outside the territory of India in cases where data of Indian residents is processed by entities who do not have any presence in India?

Ans. Similar to EU GDPR model.

Clause (1) states that the regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the Union.

Clause (2) widens the reach of the regulation by making it applicable to processing of personal data of data subjects who are in Indian territory by controllers and processors outside the Indian territory, if the processing activities are related to the

offering of goods and services to persons in the Indian territory or if the behaviour of such persons in the Indian territory is monitored by such activities

It should be done through bi-lateral treaties.

3. While providing such protection, what kind of link or parameters or business activities should be considered?

Response: Regulate entities which offer goods or services in India even though they may not have a presence in India. As quoted in Clause 2 in above questions.

4. What measures should be incorporated in the law to ensure effective compliance by foreign entities inter alia when adverse orders (civil or criminal) are issued against them?

Response The country should expand itself in cyber diplomacy through bilateral talks across borders. Access to Indian market is blocked if they don't have compliance with the law.

5. Are there any other views on the territorial scope and the extra-territorial application of a data protection law in India , other than the ones considered above?

Response. Manual collection of data should be covered under the act. For instance, Scanning of Aadhar, KYC for banks.

Chapter 2. Other Issues of Scope

There are three issues of scope other than territorial application. These relate to the applicability of the law to data relating to juristic persons such as companies, differential application of the law to the private and the public sector, and retrospective application of the law.

Questions

1. What are your views on the issues relating to applicability of a data protection law in India in relation to: (i) natural/juristic person; (ii) public and private sector; and (iii) retrospective application of such law?

Response: (i) Provisional view stated is :

“Given prevalent best practices, the law may apply to natural persons only. The primary object of the legislation being to protect the informational privacy right of an individual, the proposed law may not be extended to include data relating to companies and other juristic entities.”

We are of the view that it should include both natural and juristic person.

(ii) There is no difference between public and private sector. Both should be treated equally under the law.

(iii) Any kind of breach of data that happens on the retrospective collection of data will fall under the law. Any breaches that have already happened in the past.

2. Should the law seek to protect data relating to juristic persons in addition to protecting personal data relating to individuals?

Alternatives:

Response: The law could regulate data of natural persons and juristic persons.

3. Should the law be applicable to government/public and private entities processing data equally? If not, should there be a separate law to regulate government/public entities collecting data?

Alternatives:

a. Have a common law imposing obligations on Government and private bodies as is the case in most jurisdictions. Legitimate interests of the State can be protected through relevant exemptions and other provisions.

Response: A, the law should treat both equally.

4. Should the law provide protection retrospectively? If yes, what should be the extent of retrospective application? Should the law apply in respect of lawful and fair processing of data collected prior to the enactment of the law?

Alternatives:

a. The law should be applicable retrospectively in respect of all obligations. b. The law will apply to processes such as storing, sharing, etc. irrespective of when data was collected while some requirements such as grounds of processing may be relaxed for data collected in the past.

Response: Option A, As No relaxation on data previously collected.

5. Should the law provide for a time period within which all regulated entities will have to comply with the provisions of the data protection law?

Response: Yes, adequate time period should be given for implementing the provisions of the time for compliance after due assessments.

6. Are there any other views relating to the above concepts?

Response: The draft law requires consultation with the citizens and the civic society. Adequate time should be given to all the stakeholders involved.

Chapter 3. What is Personal Data ?

The definition of personal information or personal data is the critical element which determines the zone of informational privacy guaranteed by a data protection legislation. Thus, it is important to accurately define personal information or personal data which will trigger the application of the data protection law.

Questions

1. What are your views on the contours of the definition of personal data or information?

Response: As defined in the Provisional views:

Data from which an individual is identified or identifiable/reasonably identifiable may be considered to be personal data. The identifiability can be direct or indirect.

Personal data is any data about an individual through which he/she can be identified but the committee agreed on the fact that the “person” should include both natural and juristic entities.

In addition, sensitive inferences drawn about individuals should be included in the definition as in the case of cyber physical systems where the data is captured from sensory devices in raw form may not indicate anything however the inferences may pose very serious risks to the privacy of the individuals.

2. For the purpose of a data protection law, should the term personal data‘ or personal information‘ be used?

Alternatives:

a. The SPDI Rules use the term sensitive personal information or data. b. Adopt one term, personal data as in the EU GDPR or personal information as in Australia, Canada or South Africa.

Response: a. The SPDI Rules use the term sensitive personal information or data

The use of term is very critical as both data and information need to be protected under the law.

3. What kind of data or information qualifies as personal data? Should it include any kind of information including facts, opinions or assessments irrespective of their accuracy?

Response: Sensitive personal data and sensitive inferences drawn on data involving an individual may be covered under this act.

4. Should the definition of personal data focus on identifiability of an individual? If yes, should it be limited to an identified‘, identifiable‘ or reasonably identifiable‘ individual?

Response: Identifiable term should be used in the definition of personal data of an individual because the power of computation is increasing day by day and identifiable data may become reasonably identifiable in future. This is specified by provisional view:

“Standard may have to be backed up by codes of practice and guidance notes indicating the boundaries of personal information having regard to the state of technology.”

5. Should anonymised or pseudonymised data be outside the purview of personal data? Should the law recommend either anonymisation or psuedonymisation, for instance as the EU GDPR does?

[Anonymisation seeks to remove the identity of the individual from the data, while pseudonymisation seeks to disguise the identity of the individual from data. Anonymised data falls outside the scope of personal data in most data protection laws while psuedonymised data continues to be personal data. The EU GDPR actively recommends psuedonymisation of data.]

Response: As suggested in the paper, Pseudonymised data should be included in the purview of personal data and anonymised data can be excluded.

6. Should there be a differentiated level of protection for data where an individual is identified when compared to data where an individual may be identifiable or reasonably identifiable? What would be the standards of determining whether a person may or may not be identified on the basis of certain data?

Response: No, we should not have differentiated level of protection for data where an individual is identified when compared to data where an individual may be identifiable or reasonably identifiable. As discussed in question no 4, we are not differentiating identifiable and reasonably identifiable data.

7. Are there any other views on the scope of the terms personal data‘ and personal information‘, which have not been considered?

Response: Personal data should included sensitive personal data and sensitive inferences drawn from it.

Chapter 4. Definition of Sensitive Personal Data

While personal data refers to all information related to a person's identity, there may be certain intimate matters in which there is a higher expectation of privacy. Such a category widely called 'sensitive personal data' requires precise definition.

Questions

Q1. What are your views on sensitive personal data?

Response: Sensitive personal data which needs to be protected may include

1. Identity information such as AADHAR card number, PAN etc.
2. financial data such as credit card/debit card information, insurance information, bank accounts.
3. sexual orientation, mental and health information, caste and religion information.
4. political views/expression and voting details.

Any other definition (data related to national security) can be incorporated based on recommendation by central govt. as prescribed by the governing/administering body.

2. Should the law define a set of information as sensitive data? If yes, what category of data should be included in it? E.g. Financial Information / Health Information / Caste / Religion / Sexual Orientation. Should any other category be included?

Response: Yes, it should include financial information, sexual orientation, mental and health information, caste and religion information. As in EU GDPR, the law should incorporate racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.

3. Are there any other views on sensitive personal data which have not been considered above?

Response: Committee agrees with all the provisional views. Its specified in provisional view that caste information may also be treated as sensitive personal data.

Chapter 5. Definition of Processing

Data protection laws across jurisdictions have defined the term processing in various ways. It is important to formulate an inclusive definition of processing to identify all operations, which may be performed on personal data, and consequently be subject to the data protection law.

Questions

1. What are your views on the nature and scope of data processing activities?

Response: Processing should include all kind of activities that can be performed over personal data whether it is in automated or manual processing. It includes collection, sharing, altering, manipulation, updating, recording, Destroying and combining of data. Definition of processing should specify all operations and activities applicable to data such as collection, use and disclosure. The definition need to be specific.

2. Should the definition of processing list only main operations of processing i.e. collection, use and disclosure of data, and inclusively cover all possible operations on data?

Response: The definition need to be specific as well as entire lifecycle of data processing (Creation, Storage, Usage include Analysis, Sharing, Archiving, Destroying) should be covered. Definition of processing should specify major operations and activities applicable to data such as collection, use and disclosure. It should be more precise when conditions for collection, use and disclosure are separately listed.(as Canada and Australia approach).

3. Should the scope of the law include both automated and manual processing? Should the law apply to manual processing only when such data is intended to be stored in a filing system or in some similar structured format?

Alternatives:

- a. All personal data processed must be included, howsoever it may be processed.
- b. If data is collected manually, only filing systems should be covered as the risk of profiling is lower in other cases.
- c. Limit the scope to automated or digital records only.

Response: Both manual and automated data processing.

4. Are there any other issues relating to the processing of personal data which have not been considered?

Response:.. The act should define all data related operations properly with scopes for additions.

Chapter 6: Entities to be defined in the law : Definition of Data Controller and Processor

The obligations on entities in the data ecosystem must be clearly delineated. To this end a clear conceptual understanding of the accountability of different entities which control and process personal data must be evolved.

Questions

Q1. What are your views on the obligations to be placed on various entities within the data ecosystem?

Response: Firstly, it should clearly identify various entities involved in data processing so to demarcate the responsibilities. For data processor and third party there should be written contracts which should include standard clauses given by data protection authorities. They should be allocated precisely their responsibility over processing of data. Data Controller should have higher accountability.

Most importantly legally binding the data broker to the data controllers is very important as Data brokers collect a huge volume of detailed information on hundreds of millions of consumers which is further sold in raw or processed form and sensitive inferences are drawn by third parties.

Q2. Should the law only define ‘data controller’ or should it additionally define data processor’?

Alternatives:

a. Do not use the concept of data controller/processor; all entities falling within the ambit of the law are equally accountable. b. Use the concept of ‘data controller’ (entity that determines the purpose of collection of information) and attribute primary responsibility for privacy to it. c. Use the two concepts of ‘data controller’ and ‘data processor’ (entity that receives information) to distribute primary and secondary responsibility for privacy.

Response. It should follow both b and c options. Use the concept of ‘data controller’ (entity that determines the purpose of collection of information) and attribute primary responsibility for privacy to it. It should use two concepts of data controller and data processor to distribute primary and secondary responsibility for privacy.

Most importantly legally binding the data broker to the data controllers is very important as Data brokers collect a huge volume of detailed information on hundreds of millions of consumers which is further sold in raw or processed form and sensitive inferences are drawn by third parties

3. How should responsibility among different entities involved in the processing of data be distributed?

Response. All options as mentioned should be included as below

- a. Making data controllers key owner and making them accountable.
- b. Clear bifurcation of roles and associated expectations from various entities.
- c. Defining liability conditions for primary and secondary owners of personal data.
- d. Dictating terms/clauses for data protection in the contracts signed between them.
- e. Use of contractual law for providing protection to data subject from data processor.

4. Are there any other views on data controllers or processors which have not been considered above?

Response. Accountability of both data controller and processor at all stages of data handling. Technological means for Traceability of data controller could be considered as well as unnecessary collection of data must be avoided.

Most importantly legally binding the data broker to the data controllers is very important as Data brokers collect a huge volume of detailed information on hundreds of millions of consumers which is further sold in raw or processed form and sensitive inferences are drawn by third parties

Chapter 7. Exemptions for Household purposes, journalistic and literary purposes and research

A data controller may be exempted from certain obligations of a data protection law based on the nature and purpose of the processing activity eg. certain legitimate aims of the state. The scope of such exemptions, also recognised by the Supreme Court in Puttaswamy needs to be carefully formulated.

Questions

1. What are the categories of exemptions that can be incorporated in the data protection law?

Response. All of them.

The categories for exemption include:

- for data processed for household purposes
- for data processed for journalistic/artistic and literary purposes.
- for data processed for the purpose of academic research, statistics and historical purposes
- For data processed information collected for the purpose of investigation of a crime, and apprehension or prosecution of offenders and national security;

2. What are the basic security safeguards/organisational measures which should be prescribed when processing is carried out on an exempted ground, if any?

Response. Adequate safeguards may be incorporated in law to ensure that the data is being used for a bonafide purpose, and has been lawfully obtained. The law must provide for adequate security and organizational safeguards in the handling of such data.

Domestic /Household Processing

1. What are your views on including domestic/household processing as an exemption?
2. What are the scope of activities that will be included under this exemption?
3. Can terms such as domestic' or household purpose' be defined?
4. Are there any other views on this exemption?

A wide exemption may be provided for data processed for household purposes.

Journalistic/Artistic/ Literary Purpose

1. What are your views on including journalistic/artistic/literary purpose as an exemption?
2. Should exemptions for journalistic purpose be included? If so, what should be their scope?
3. Can terms such as 'journalist' and 'journalistic purpose' be defined?
4. Would these activities also include publishing of information by non-media organisations?
5. What would be the scope of activities included for literary' or artistic' purpose? Should the terms be defined broadly?

6. Are there any other views on this exemption?

Response: A wide liberal interpretation should be taken which protects right to free speech as envisaged by our constitution.

Journalistic:

- Non media should be kept out.
- Rules for publishing the information (can be distributed further)
- Publishing with anonymity.
- Comments from the public can be taken.

Research/Historical/Statistical Purpose

1. What are your views on including research/historical/statistical purpose as an exemption?

Response: Should be exempted.

2. Can there be measures incorporated in the law to exclude activities under this head which are not being conducted for a bonafide purpose?

Response: YES

3. Will the exemption fail to operate if the research conducted in these areas is subsequently published/ or used for a commercial purpose?

Response: YES if prior permission has not been taken for the same.

4. Are there any other views on this exemption?

NIL

What are your views on including investigation and detection of crimes and national security as exemptions?

Response: Should be exempted.

2. What should be the width of the exemption provided for investigation and detection of crime? Should there be a prior judicial approval mechanism before invoking such a clause?

Response: In case of a Public emergency a judicial review in a prescribed timeframe should be mandated. Otherwise a prior judicial approval mechanism should be invoked.

3. What constitutes a reasonable exemption on the basis of national security? Should other related grounds such as maintenance of public order or security of State be also grounds for exemptions under the law?

Response: YES

4. Should there be a review mechanism after processing information under this exemption? What should the review mechanism entail?

Response: YES, judicial review in a prescribed timeframe.

5. How can the enforcement mechanisms under the proposed law monitor/control processing of personal data under this exemption?

Response: Technicl means to be incorporated for the same.

6. Do we need to define obligations of law enforcement agencies to protect personal data in their possession?

Response: YES

7. Can a data protection authority or/and a third-party challenge processing covered under this exemption?

Response: YES

8. What other measures can be taken in order to ensure that this exemption is used for bona fide purposes?

Response: YES, judicial review in a prescribed timeframe.

9. Are there any other views on these exemptions?

Response: NIL

The law may provide exemptions for the following purposes/processing activities: (i) information collected for the purpose of investigation of a crime, and apprehension or prosecution of offenders; (ii) information collected for the purpose of maintaining national security and public order.

Additional Exemptions

1. Should prevention of crime be separately included as ground for exemption?

Response: YES, with prior judicial permission.

2. Should a separate exemption for assessment and collection of tax in accordance with the relevant statutes be included?

Response: YES, with prior judicial permission

3. Are there any other categories of information which should be exempt from the ambit of a data protection law?

Response: The exemptions must be defined in a manner to ensure that processing of data under the exemptions is done only for the stated purpose. Further, it must be demonstrable that the data was necessary for the stated purpose.

Chapter 8. Cross Border Flow of Data

Given the advent of the Internet, huge quantities of personal data are regularly transferred across national borders. Providing strong rules to govern such data flows is vital for all entities in the data eco-system.

Questions

1. What are your views on cross-border transfer of data?

Response: According to provisional view given “There are two tests identified for formation of laws related to cross border data flow, namely the adequacy test and the comparable level of protection test for personal data. In order to implement the adequacy test, there needs to be clarity as to which countries provide for an adequate level of protection for personal data.”

Cross-border flow of data is vital to accessing valuable digital services. Providing strong rules to protect cross-border data flows is crucial for small and medium sized enterprises or SMEs, consumers, and multi-national businesses. Data controller should be the one who is collecting the data and the company, which is giving services in India, should be forced to process and store the data created from India locally in India. Anonymized data can flow cross borders through bi-lateral treaties which need to be negotiated.

2. Should the data protection law have specific provisions facilitating cross border transfer of data? If yes, should the adequacy standard be the threshold test for transfer of data?

Response: Under the Data protection law, Sensitive data should not be transferred across Indian border in of the case. Anonymized data can flow cross borders through bi-lateral treaties, which need to be negotiated.

3. Should certain types of sensitive personal information be prohibited from being transferred outside India even if it fulfils the test for transfer?

Response: All sensitive personal information should be prohibited from being transferred outside India

4. Are there any other views which have not been considered?

Response: Govt. of India should encourage and rather mandate indigenous technology especially for CI. Infrastructure, scope, requirements (hardware, software) need to be framed and defined.

Chapter 9. Data Localisation

Data localisation requires companies to store and process data on servers physically located within national borders. Several governments, driven by concerns over privacy, security, surveillance and law enforcement, have been enacting legislations that necessitate localisation of data. Localisation measures pose detrimental effects for companies may, harm Internet users, and fragment the global Internet.

Questions

1. What are your views on data localisation?

Personal Data should be localized. A localised data centre will certainly prove to be an effective tool for security agencies. It will help prevent diplomatic delays and denials due to which investigation gets hindered. Also, this can prevent our citizens from getting economically exploited by developed nations. Having a technological backbone made up of Cloud Service providers, Analytics Ecosystems, Cyber Physical Systems, IOT, Artificial Intelligence and Big data will definitely make us self reliant.

In 2016, **Colombia's Ministry of Information and Communication Technology** publicly called for data localization and released a document—on “Basic Digital Services”—that recommends that data-processing centres should be in Colombia, as they perceive storing data overseas to be too great a risk to network security and personal data. Furthermore, there are concerns that Colombia's National Procurement Office (NPO) may include data localization requirements or other barriers to data flows as part of a cloud services procurement project for government agencies. Early drafts show the NPO is considering a vague and arbitrary “adequacy” assessment to decide which countries provide adequate data protection. The NPO has reportedly prepared a draft list of “adequate” countries, which does not include the United States, without detailing how these countries were assessed.

Two Canadian provinces, British Columbia and Nova Scotia, have implemented laws mandating that personal data held by public bodies such as schools, hospitals, and public agencies must be stored and accessed only in Canada, unless certain conditions are fulfilled. The tender for the project to consolidate the federal government's ICT services, including email, for 63 different agencies requires the contracting company to store the data in Canada (citing national security reasons).

China

- China enacted a new cybersecurity law that forces a broad range of companies to store users' personal information and other important business data in China.
- In March 2016, China enacted new regulations regarding cloud-computing services in China that essentially exclude foreign technology firms and reinforce local data-storage requirements.

- In April 2017, China released a draft circular that outlined extensive localization requirements—both explicit and implicit—as part of a restrictive regime of “security checks” for businesses wanting to transfer data overseas, further to the cybersecurity law, which outlined the need for such security assessments. This draft extends data localization from “critical information infrastructure” to all “network operators,” which is likely any owner or administrator of a computerized information network system. Furthermore, any outbound data transfer would be prohibited if it brings risks to the security of the national political system, economy, science and technology or national defines.”The EU’s law on personal data protection only allows for the transfer of such data to third countries outside the EU that it has determined provide an “adequate” level of protection. So far, the EU has only recognized 12 countries: Andorra, Argentina, Canada, Switzerland, the Faeroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, the United States (through the U.S.-EU Privacy Shield Framework), and Uruguay. Data Localisation and regulation of cross border data flows will definitely help the cause in preserving individual’s privacy and especially from national security perspective. We recommend that Clear individual rights, fair information practises should be incorporated in the Law.

2. Should there be a data localisation requirement for the storage of personal data within the jurisdiction of India?

Response: Yes

Q3. If yes, what should be the scope of the localisation mandate? Should it include all personal information or only sensitive personal information?

Response: Flow of personal information should be done through Bilateral treaties after Security assessment. However flow of sensitive personal information should be strictly prohibited.

Q4. If the data protection law calls for localisation, what would be impact on industry and other sectors?

Response:

Foreign Investment will hugely increase if we implement a law of Data Localization.

Data localization means a complete paradigm shift in the way an MNC will function within the boundaries of India. The MNCs will have to change the existing architecture and their production processes. The following are the major changes that will occur and will also bring in a lot of Foreign Investment in the country:

1. Data Centres in India:

If such a practise comes into place, the foreign Investment firms will need to set up their data centres within the territory of India. New data centres mean

newer opportunities for the Indian IT skilled professionals. Large-scale employment will be generated for the Indian Manpower, which further will enhance the existing business and bring in more capital. Incremental data centres requirements will also be catered in India.

2. Technology Sharing:

A lot of Technology will also flow into India.

3. Process and Standardization:

Managing the technology and data centres will require standards to come into place. Structured processes will be followed which in turn will make the system more efficient and progressive. Standardization will also ensure uniformity.

4. Transformation Projects In-Flow:

If a law like Data Localization comes into place, then a lot of personal data of the Indian Residents will be demanded back into the Indian borders. Hence, a large scope for a having domestic data transformation projects. Many MNCs will be compelled to start with migration projects which in turn will fetch a lot of capital. A lot of employment will be generated too.

5. Entire project lifecycle processes in the National Boundary:

As many stages of a project will be undertaken in India, this will bring in a lot of monetary benefits to India.

6. Boost to Indigenous technology:

The government will be motivated to setup an in-house IT industry and start-up sector focusing on development of Indigenous technology. This will lure the foreign VCs to invest in India.

7. Lifecycle Management & Maintenance Projects:

Entire lifecycle and maintenance of the data centres and related projects will require skilled labour. It will also bring in a lot of FDI.

Q5. Are there any other issues or concerns regarding data localisation which have not been considered above?

Response: It will increase the foreign investments

Chapter 10. Allied Laws

Views on Financial Sector Laws:

Views
<p>There is a need for clauses that specify the Banking information that a bank needs to retain and share with other banks and in what format, encryption mechanisms.</p> <p>Sharing customer data also must require detailed explanation and reasoning.</p> <p>Static and Transactional data must have proper definitions and thus, proper security policies in place.</p>
<p>Policies for data protection need to come into place.</p> <p>The credit/CIBIL information of a customer needs to be protected.</p> <p>Rules at API levels need to be formulated so that only the required information is accessed</p>
<p>The information stored by this regulatory body must frame rules for access to data of defaulters, persons and utilities.</p>
<p>The payment information like account number, gateway data must be protected when it is stored or used during transactions.</p> <p>What information needs to be stored should also be lawfully guided.</p>
<p>KYC information and credit card information if stored centrally in a localized fashion, then only the part of it needed by third parties should be made accessible instead of providing full access.</p> <p>Each type of access must be verified and reasoned thoroughly.</p> <p>Need for API design and laws</p>
<p>Protection of data is required, Credentials be protected</p>
<p>Insurance companies need to explain how and why do they require to use a customer's data for commercial/exploratory purposes.</p> <p>Companies must be held accountable for the data that they exploit.</p> <p>The customer must also be made aware of the data being used.</p>

Views on Health Sector:

<p>Medical records must be protected.</p> <p>Strict laws for misusing this data without consent.</p>
--

Medical data must be categorized into severity and sensitivity levels and each level must have defined rules for transfer/sharing.

Views on Telecomm and IT sector:

Rules for sharing CDRs, sensitive data and location.
Define Geographical boundaries for data exchanges.
Regulations for storing data on cross border servers
Rules for better encryption.

Other Views:

Rules for sharing
Should not be easily available for commercial use
As far as possible involve indigenous companies
Stringent laws for crimes like Identity theft

Demographic data needs to be protected
Regulation of data that is used publicly

Laws on what kind of information can be collected
Sample surveys need to be checked

Consumers should be protected against exploitation of their data
Rules for consent

Need for amendments to what digital information can be asked for
MNCs need to be included in the RTI list

GROUNDS OF PROCESSING, OBLIGATION ON ENTITIES AND INDIVIDUAL RIGHTS

Chapter 1: Consent

Most jurisdictions treat consent as one of the grounds for processing of personal data. However, consent is often not meaningful or informed, which raises issues of the extent to which it genuinely expresses the autonomous choice of an individual. Thus, the validity of consent and its effectiveness needs to be closely examined.

Questions

- 1. What are your views on relying on consent as a primary ground for processing personal data?**

Alternatives:

- a. Consent will be the primary ground for processing.
- b. Consent will be treated at par with other grounds for processing.
- c. Consent may not be a ground for processing.

Response: Option A i.e. having consent as the primary ground for processing of personal information as it allows information privacy.

But there should be exceptions on national security and criminal exceptions which need to be specified explicitly.

- 2. What should be the conditions for valid consent? Should specific requirements such as “unambiguous”, “freely given” etc. as in the EU GDPR be imposed? Would mandating such requirements be excessively onerous?**

Response: Ask organisations or data controllers to explicitly mention the terms and conditions in their notices about the third parties or data brokers to which they will share the user's data.

- 3. How can consent fatigue and multiplicity of notices be avoided? Are there any legal or technology-driven solutions to this?**

Response: The notice should be granular. A person should be able to exercise choices on different conditions listed.

- 4. Should different standards for consent be set out in law? Or should data controllers be allowed to make context-specific determinations?**

Response: The panel has agreed on having context-specific determinations as the different contexts have different ways of functioning, each requires a different handling mechanism

- 5. Would having very stringent conditions for obtaining valid consent be detrimental to day-to-day business activities? How can this be avoided?**

Response: Cannot be avoided

- 6. Are there any other views regarding consent, which have not been explored above?**

Response: The consent taken from a data subject must be valid for a specific time frame, after which the consent need to be retaken and subject should be allowed to change one's consent choice.

Chapter 2. Child's Consent

It is estimated that globally, one in three Internet users is a child under the age of 18. Keeping in mind their vulnerability and increased exposure to risks online, a data protection law must sufficiently protect their interests.

Questions

1. **What are your views regarding the protection of a child's personal data?**

Response: The person taking decision about his/her information should be at least 14 years of age with a minimum intellectual ability.

2. **Should the data protection law have a provision specifically tailored towards protecting children's personal data?**

Response: Yes, the data protection law must have a provision specifically tailored towards protecting children's protection data and to prevent child abuse.

3. **Should the law prescribe a certain age-bar, above which a child is considered to be capable of providing valid consent? If so, what would the cut-off age be?**

Response: A child is considered to be capable of providing valid consent after the age of 14 as he gets adequate intellectually able at this age to be able to use digital media.

4. **Should the data protection law follow the South African approach and prohibit the processing of any personal data relating to a child, as long as she is below the age of 18, subject to narrow exceptions?**

Response: The child below the age of 14 should be considered for the above statement.

5. **Should the data protection law follow the Australian approach, and the data controller be given the responsibility to determine whether the individual has the capacity to provide consent, on a case by case basis? Would this requirement be too onerous on the data controller? Would relying on the data controller to make this judgment sufficiently protect the child from the harm that could come from improper processing?**

Response: The consent should be given by parents. When parents do not have required knowledge, it should be decided on case by case basis, which can be different for every child.

6. **If a subjective test is used in determining whether a child is capable of providing valid consent, who would be responsible for conducting this test?**

Alternatives:

- a. The data protection authority
- b. The entity which collects the information
- c. This can be obviated by seeking parental consent

Response: The panel agreed on two alternatives 'a' and 'c' because if the test is conducted by the entity collecting the information, it may take a biased decision in their own interest.

7. **How can the requirement for parental consent be operationalised in practice? What are the safeguards which would be required?**

Response: Identity of parents should be taken and verified for parental consent to be operationalised.

8. **Would a purpose-based restriction on the collection of personal data of a child be effective? For example, forbidding the collection of children's data for marketing, advertising and tracking purposes?**

Response: Children's personal data should not be allowed to be process even if it is collected under some purpose based restriction

9. **Should general websites, i.e. those that are not directed towards providing services to a child, be exempt from having additional safeguards protecting the collection, use and disclosure of children's data? What is the criteria for determining whether a website is intended for children or a general website?**

Response: These websites should not be exempted for having additional safeguards to protect the collection use and disclosure of children's data.

10. **Should data controllers have a higher onus of responsibility to demonstrate that they have obtained appropriate consent with respect to a child who is using their services? How will they have –actual knowledgell of such use?**

Response: Yes, data controllers should have responsibility to demonstrate that they have obtained appropriate consent in the cases whenever required.

11. **Are there any alternative views on the manner in which the personal data of children may be protected at the time of processing?**

-----None

Chapter 3: Notice

Notice is an essential prerequisite to operationalise consent. However, concerns have been raised about notices being ineffective because of factors such as length, use of complex language, etc. Thus, the law needs to ensure that notices are effective, such that consent is meaningful.

Questions

1. Should the law rely on the notice and choice mechanism for operationalising consent?

Response: Yes, Organisations should provide consent to process personal information and how that information has been used. So, it is a good mechanism for operationalising consent. Mandatory notice is a popular form of privacy self-management, which plays a role in most data protection laws. Both email and sms should be mandatory mechanisms for sending the notice though additional modes if need be can also be adopted.

2. How can notices be made more comprehensible to individuals? Should government data controllers be obliged to post notices as to the manner in which they process personal data?

Response: Notice should be comprehensible to individuals addressing difficulties relating to notice readability, comprehension and access, by providing that it must contain clear explanations, language at an appropriate reader level. Yes, government data controllers should be obliged to post notices as to the manner in which they process personal data.

3. Should the effectiveness of notice be evaluated by incorporating mechanisms such as privacy impact assessments into the law?

Response: Yes, there should be a mechanism to evaluate the effectiveness of the notice e.g. Privacy Impact Assessment tools mentioned in provisional views. This will also be helpful in case there are any issues between the end users and the firm to which notice belongs. And also the transparency of the terms and conditions will be evaluated. But, it should be formulated keeping Indian context in mind.

4. Should the data protection law contain prescriptive provisions as to what information a privacy notice must contain and what it should look like?

Response: Option b

Form based requirements may be prescribed by sectorial regulators or by the data protection authority in consultation with sectorial regulators.

5. How can data controllers be incentivised to develop effective notices?

Alternatives:

- a. Assigning a data trust score
- b. Providing limited safe harbour from enforcement if certain conditions are met.

If a data trust score is assigned, then who should be the body responsible for providing the score?

Response: Incentivisation for data controllers is not so necessary.

6. Would a consent dashboard be a feasible solution in order to allow individuals to easily gauge which data controllers have obtained their consent and where their personal data resides? Who would regulate the consent dashboard? Would it be maintained by a third party, or by a government entity?

Response: Yes, if the original data controller has passed an individual's personal information to any other third party, the individual must know where his/her data is residing and details of data controllers/third party processors/parties with whom the information has been shared. It should be regulated by a government entity or a data protection authority.

7. Are there any other alternatives for making notice more effective, other than the ones considered above?

Response: No

Chapter 4: Other Grounds of Processing

It is widely recognised that consent may not be sufficient as the only ground for lawful processing of personal data. Several other grounds, broadly conforming to practical requirements and legitimate state aims, are incorporated in various jurisdictions. The nature and remit of such grounds requires determination in the Indian context.

Questions

1. What are your views on including other grounds under which processing may be done?

Response: Consent is sponsored and might not be correct. Legitimate and vital interest should be legally defined.

2. What grounds of processing are necessary other than consent?

Response: In cases of life threatening conditions/emergencies.

3. Should the data protection authority determine residuary grounds of collection and their lawfulness on a case-by-case basis? On what basis shall such determination take place?

Alternatives:

- a. No residuary grounds need to be provided.
- b. The data protection authority should lay down lawful purposes by means of a notification.
- c. On a case-by-case basis, applications may be made to the data protection authority for determining lawfulness.
- d. Determination of lawfulness may be done by the data controller subject to certain safeguards in the law.

Response: Option C - Data protection authorities can be different in each state. This can be taken care on case to case basis as it will consider and compensate for cultural differences as well.

4. Are there any alternative methods to be considered with respect to processing personal data without relying on consent?

Response: There has to be provision in laws to govern certain types of personal data processing wherein informed consent is not possible.

Chapter 5: Purpose Specification And Use Limitation

1. What are your views on the relevance of purpose specification and use limitation principles?

Response: It should be specified.

2. How can the purpose specification and use limitation principles be modified to accommodate the advent of new technologies?

Response: As and when it comes.

3. What is the test to determine whether a subsequent use of data is reasonably related to/ compatible with the initial purpose? Who is to make such determination?

Response: No test required.

4. What should the role of sectorial regulators be in the process of explicating standards for compliance with the law in relation to purpose specification and use limitation?

Response: Point b

5. Are there any other considerations with respect to purpose specification and use limitation principles which have not been explored above?

Response: No Response

Chapter 6: Processing Of Sensitive Personal Data

1. **What are your views on how the processing of sensitive personal data should be done?**

Response: Under no circumstances personal sensitive data should be allowed to leave the country. Under all circumstances, privacy of the individual needs to be preserved. Exemptions as prescribed in law may be applicable.

2. **Given that countries within the EU have chosen specific categories of –sensitive personal data, keeping in mind their unique socio-economic requirements, what categories of information should be included in India’s data protection law in this category?**

Response: Categories previously specified in Chapter II may be considered

3. **What additional safeguards should exist to prevent unlawful processing of sensitive personal data?**

Response: EU GDPR Model needs to be followed which has very precisely described the way to prevent unlawful processing of sensitive personal data

4. **Should there be a provision within the law to have sector specific protections for sensitive data, such as a set of rules for handling health and medical information, another for handling financial information and so on to allow contextual determination of sensitivity?**

Response: Yes

5. **Are there any alternative views on this which have not been discussed above?**

Response: NA

Chapter 7: Storage Limitation And Data Quality

1. **What are your views on the principles of storage limitation and data quality?**

Response: It should be maintained and not compromised at all during the entire lifecycle of the data.

2. **On whom should the primary onus of ensuring accuracy of data lie especially when consent is the basis of collection?**

Alternatives:

- a. The individual
- b. The entity collecting the data

Response: Responsibility of providing accurate data lies on an individual while accuracy of data while processing and storing lies on the entity collecting the data

3. **How long should an organisation be permitted to store personal data? What happens upon completion of such time period?**

Response: Time for storing of personal data should be specified at the time of collection of data. After completion of such time period, the personal data should be securely erased and due notice should be given to the data subject.

4. **If there are alternatives to a one-size-fits-all model of regulation (same rules applying to all types of entities and data being collected by them) what might those alternatives be?**

Response: No

5. **Are there any other views relating to the concepts of storage limitation and data quality which have not been considered above?**

Response: Need to have Indian standard for data quality. Quality of data should not be compromised during the lifecycle of the data processing. It should be the responsibility of the data controller/processor to ensure the same.

Chapter 8: Individual Participation Rights-1

1. What are your views in relation to the above?

Response:

- A person should be made aware of the usage of the personal information that he has submitted to a data controller.
- All types of direct/indirect commercial usage of a user's personal data must be reported to a user and he should have full right over the processing of this data.
- No fee should be charged to a data subject in case he/she files a rectification request.

2. Should there be a restriction on the categories of information that an individual should be entitled to when exercising their right to access?

Response: The individual should not be subjected to any restrictions while exercising his/her right.

3. What should be the scope of the right to rectification? Should it only extend to having inaccurate data rectified or should it include the right to move court to get an order to rectify, block, erase or destroy inaccurate data as is the case with the UK?

Response: Inaccurate, outdated, misleading Personal information shall fall under the scope of right to rectification.

Firstly, it should provide the right to get the data rectified from the data controller. In the case of denial by the data operator to rectify, should there be a provision for the data subject to move to court.

4. Should there be a fee imposed on exercising the right to access and rectify one's personal data?

Alternatives:

- a. There should be no fee imposed.
- b. The data controller should be allowed to impose a reasonable fee.
- c. The data protection authority/sectorial regulators may prescribe a reasonable fee.

Response: There should be no fee imposed.

5. Should there be a fixed time period within which organisations must respond to such requests? If so, what should these be?

Response: Yes there should be a time limit of 15 days within which organisations must respond to such requests.

6. Is guaranteeing a right to access the logic behind automated decisions technically feasible? How should India approach this issue given the challenges associated with it?

Response: Yes, since it is also well stated in the policies of EU, United Kingdom on grounds that the automated decision may affect an individual.

India should also device a policy similar to the EU in this regard.

7. What should be the exceptions to individual participation rights? [For instance, in the UK, a right to access can be refused if compliance with such a request will be impossible or involve a disproportionate effort. In case of South Africa and Australia, the exceptions vary depending on whether the organisation is a private body or a public body.]

Response: The panel recommends that no exceptions should be made to the personal data of a data subject.

8. Are there any other views on this, which have not been considered above?

Response: A strong recommendation by the panel is that no fee should be charged to the data subject for making a rectification request.

The data controller may also be held accountable in case a data is found to be incorrect, misleading about an individual.

Chapter 9: Individual Participation Rights – II

1. What are your views on the above individual participation rights?

Response:

- Each person should have complete control over the data shared by him with a data operator.
- He should have all the right to know where is the data being used, processed for commercial purposes.
- He should have the right to interject in case of an automated decision supplied by AI solution pertaining to his data.
- Processing of personal data for direct marketing purposes may be recognized as a discrete privacy principle in a data protection law for India.
- The individual has the right to object to processing, on reasonable grounds, if the basis of processing was:
 - protection of legitimate interest of the individual,
 - proper performance of public law duty by a public body,
 - pursuit of legitimate interest of the organization.

2. The EU GDPR introduces the right to restrict processing and the right to data portability. If India were to adopt these rights, what should be their scope?

Response: India should adopt the right to data portability according to the EU mandate so that the individual is not locked within the service of one operator. The EU GDPR states that:

“The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and the processing is carried out by automated means.”

3. Should there be a prohibition on evaluative decisions taken on the basis of automated decisions?

Alternatives:

- a. There should be a right to object to automated decisions as is the case with the UK.

- b. There should a prohibition on evaluative decisions based on automated decision making.

Response: Yes, EU model should to be followed and there should be a right to object to automated decisions

4. Given the concerns related to automated decision making, including the feasibility of the right envisioned under the EU GDPR, how should India approach this issue in the law?

Response: The panel recommends that the EU GDPR rights be incorporated. It states that:

“The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.”

5. Should direct marketing be a discrete privacy principle, or should it be addressed via sector specific regulations?

Response: Yes, it should be a discrete privacy principle,

6. Are there any alternative views which have not been considered?

Response: The EU GDPR model is a good model to be followed in this context.

Chapter 10: Individual Participation Rights III - Right to Be Forgotten

1. What are your views on the right to be forgotten having a place in India 's data protection law?

Response:

- Such a right must be there subjected to exceptional cases like auditing, event log maintenance where the data operator must keep data for sometime for investigative purposes.
- Data should be taken down from the website and there should be a particular time period, after which that data should be deleted from the data controller.
- 120 days should be the time given to the data controller to delete it permanently

2. Should the right to be forgotten be restricted to personal data that individuals have given out themselves?

Response: The panel recommends that the right be restricted to personal data that individuals have given out themselves.

3. Does a right to be forgotten add any additional protection to data subjects not already available in other individual participation rights?

Response: Yes it definitely compliments the other rights.

4. Does a right to be forgotten entail prohibition on display/dissemination or the erasure of the information from the controller 's possession?

Response:

- Yes, it does prohibit the controller from display or erase a user's data without their consent.
- The right protects the data of a user from unnecessary being displayed at platforms unknown to the user and his data being used without consent.
- A user sharing his data with a controller must be in full possession of his data and its usage even when lying with a third party.

5. Whether a case-to-case balancing of the data subject 's rights with controller and public interests is a necessary approach for this right? Who should perform this balancing exercise? If the burden of balancing rests on the data controller as it does in the EU, is it fair to also impose large penalties if the said decision is deemed incorrect by a data protection authority or courts?

Response: Yes, as mentioned in the EU GDPR.

6. Whether special exemptions (such as the right to freedom of expression and information) are needed for this right? (over and above possible general exemptions such as national security, research purposes and journalistic or artistic expression)?

Response: No, the only exceptions to be made should be:

- National Security
- Research purposes
- Journalistic or artistic expressions

7. Are there any alternative views to this.

Response: A provision for maintaining a data subjects' data for a period of 120 days must be included. After this, the data should be removed from all places.

REGULATION AND ENFORCEMENT

Chapter 1: Enforcement Models

1. What are your views on the above described models of enforcement?

Response: The committee suggested that a co-regulated approach must be followed to formulate standards and laws for the Data Controllers. A self regulatory model should be adhered to for the regulation & compliance of standards. And lastly, if a Data Controller is found to be non compliant then the command and control enforcement model should come into place for penalties.

2. Does co-regulation seem an appropriate approach for a data protection enforcement mechanism in India?

Response: Same as given in question 1.

3. What are the specific obligations/areas which may be envisaged under a data protection law in India for a

(i) command and control approach;

(ii) self-regulation approach (if any); and

(iii) co-regulation approach?

Response: (i) command and control approach: When Data Controller is found to be Non Compliant

(ii) self-regulation approach (if any): At the implementation stage by a Data Controller

(iii) co-regulation approach: To formulate the policies (to get an industry perspective)

4. Are there any alternative views to this?

Response: Same response as in Question 1

Chapter 2: Accountability and Enforcement Tools

Accountability

1. What are your views on the use of the principle of accountability as stated above for data protection?

Response: The committee agreed to the provisional views given in the paper. The committee was of the opinion that in a case of multiple data controllers, anyone down the chain who is given access to the data should take care to ensure that it does not result in any harm to a data subject.

2. What are the organizational measures that should be adopted and implemented in order to demonstrate accountability? Who will determine the standards which such measures have to meet?

Response:

- The data controller, before commencing such processing, must consider the relevant standards in the law which apply to the processing.
- The standards may include requirements relating to grounds of processing, notice, consent, data quality, security of collected data, questions of access to data when data is to be handled by a data processor, etc.
- The data controller must draw up a procedure or policy as to how it intends to meet these standards.
- The data controller may also take into account any voluntary standard beyond the baseline norm which it abides by.
- If harm is caused to an individual owing to such processing, the data controller will bear the burden of proof to demonstrate that it had a policy to prevent such harm and implemented such policy.
- If such a policy does not exist, or was not implemented strictly, the data controller would be liable for damages.

Determination of standards must be the responsibility of a Data Protection agency.

3. Should the lack of organizational measures be linked to liability for harm resulting from processing of personal data?

Response: Yes, it must be linked. An organization must ensure security safeguard obligations such as External, Internal audits, training the staff, risk assessment and mitigation planning. Organizational measures are one of the responsibilities of an organization.

4. Should all data controllers who were involved in the processing that ultimately caused harm to the individual be accountable jointly and severally or should they be allowed mechanisms of indemnity and contractual affixation of liability inter se?

Response: All data controllers must be accountable jointly, as specified in the PIPEDA act of Canada and the EU GDPR.

5. Should there be strict liability on the data controller, either generally, or in any specific categories of processing, when well-defined harms are caused as a result of data processing?

Response: Yes, since the data controller should be held accountable for data handling at each stage of data processing.

6. Should the data controllers be required by law to take out insurance policies to meet their liability on account of any processing which results in harm to data subjects? Should this be limited to certain data controllers or certain kinds of processing?

Response: It can be a guideline but not mandated.

7. If the data protection law calls for accountability as a mechanism for protection of privacy, what would be impact on industry and other sectors?

Response: The industry needs to adapt according to the law for accountability.

8. Are there any other issues or concerns regarding accountability, which has not been considered above?

Response: EU GDPR is a good reference in this regard which requires that organizations put in place appropriate technical and organizational measures and be able to demonstrate what they did and its effectiveness when requested. Organizations, and not Data Protection Authorities, must demonstrate that they are compliant with the law. Such measures include: adequate documentation on what personal data are processed, how, to what purpose, how long; documented processes and procedures aiming at tackling data protection issues at an early state when building information systems or responding to a data breach; the presence of a Data Protection Officer that be integrated in the organization planning and operations etc.

A. Codes of Practice

1. What are your views on this?

Response: As discussed in chapter 1, The committee suggested that a co-regulated approach must be followed to formulate standards and laws for the Data Controllers. A self regulatory model should be adhered to for the regulation & compliance of standards. And lastly, if a Data Controller is found to be non compliant then the command and control enforcement model should come into place for penalties.

2. What are the subject matters for which codes of practice may be prepared?

Response: As specified in EU GDPR, codes of conduct are recognized as compliance-signaling or demonstrating tools in a number of provisions. Further provisions deal with the codes themselves stipulating that they can be formulated for subject matters like:

- a. fair and transparent processing;
- b. the legitimate interests pursued by controllers in specific contexts;
- c. the collection of personal data;
- d. the exercise of the rights of data subjects;
- e. technical and organizational measures, measures introducing data protection by design and by default, and safeguards for the security of processing;
- f. the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects; or
- g. the transfer of personal data to third countries or international organisations.

3. What is the process by which such codes of conduct or practice may be prepared? Specifically, which stakeholders should be mandatorily consulted for issuing such a code of practice?

Response: To be decided by Data Protection Authority

4. Who should issue such codes of conduct or practice?

Response: To be decided by Data Protection Authority

5. How should such codes of conduct or practice be enforced?

Response: To be decided by Data Protection Authority

6. What should be the consequences for violation of a code of conduct or practice?

Response: It should be decided on case-by-case basis and should depend on the amount of damage caused.

6. Are there any alternative views?

B. Personal Data Breach Notification

The aggregation of data in the hands of public and private entities leaves them vulnerable to data breaches. Data breaches can take many forms including; hackers gaining access to data through a malicious attack; lost, stolen, or temporary misplaced equipment; employee negligence; and policy and/or system failure. It is important to identify these threats and establish processes to deal with these breaches.

1. What are your views in relation to the above?

2. How should a personal data breach be defined?

Response: The definition of Personal data breach given in IT Act should be considered.

3. When should personal data breach be notified to the authority and to the affected individuals?

Response: The notification should be done as soon as possible

4. What are the circumstances in which data breaches must be informed to individuals?

Response: In all circumstances of data breach, the individual should be notified keeping in view that the data is somehow related to the individual

5. What details should a breach notification addressed to an individual contain?

Response: A personal data breach notification should mention:

- (i) The type of personal data breach
- (ii) The estimated date of the breach (could be in the form of a range)
- (iii) General description of the security incident in language that is comprehensible for an individual with average technical and legal knowledge.

6. Are there any alternative views in relation to the above, others than the ones discussed above?

C. Categorization of Data Controllers

Given the complexity and breadth of application of a data protection law, it may be difficult for a regulator to effectively ensure compliance on the part of all data controllers. Further, a data protection law can entail heavy compliance burdens. As a result, it may be necessary, both for principled and practical reasons to differentiate between data controllers, depending on factors that give rise to greater risks or threats to individual data protection rights.

1. What are your views on the manner in which data controllers may be categorised?

Response: The data controllers can be classified based on two factors :

- i) Annual turnover - (Australian Privacy Act classifies an organization as a small businessesll if its annual turnover AUD 3 million or less)
- ii) Risk involved with the data that they are handling

2. Should a general classification of data controllers be made for the purposes of certain additional obligations facilitating compliance while mitigating risk?

Response: Yes, a general classification of data controllers should be made for the purposes of certain additional obligations facilitating compliance while mitigating risk

3. Should data controllers be classified on the basis of the harm that they are likely to cause individuals through their data processing activities?

Response: Yes, data controllers should be classified on the basis of the harm that they are likely to cause individuals through their data processing activities

4. What are the factors on the basis of which such data controllers may be categorised?

Response: As discussed in Question: 1.

5. What range of additional obligations can be considered for such data controllers?

Response: Risk assessment can be considered as one obligation for data controllers

6. Are there any alternative views other than the ones mentioned above?

Registration

1. **Should there be a registration requirement for certain types of data controllers categorised on the basis of specified criteria as identified above? If yes, what should such criteria be; what should the registration process entail?**

Response: YES, there should be a registration requirement for certain types of data controllers categorized on the basis of specified criteria as identified above. However, It may not be made compulsory for everyone.

2. **Are there any alternative views in relation to registration?**

Data Protection Impact Assessment

1. **What are your views on data controllers requiring DPIAs or Data Protection Impact Assessments?**

Response: DPIA may not be required in all the cases

2. **What are the circumstances when DPIAs should be made mandatory?**

Response: DPIA should be made mandatory for the organisations which handle personal data of the individuals and where the risk with the breach is comparatively higher.

3. **Who should conduct the DPIA? In which circumstances should a DPIA be done (i) internally by the data controller; (ii) by an external professional qualified to do so; and (iii) by a data protection authority?**

Response: This decision has to be made by the data protection authority

4. **What are the circumstances in which a DPIA report should be made public?**

Response: DPIA report should be made public in cases where the impact may effect other organizations

5. **Are there any alternative views on this?**

Data Protection Audit

1. **What are your views on incorporating a requirement to conduct data protection audits, within a data protection law?**

Response: The data protection audit has to be carried out at least once a year.

2. **Is there a need to make data protection audits mandatory for certain types of data controllers?**

Response: Data protection Audits should be made compulsory for all the data controllers

3. **What aspects may be evaluated in case of such data audits?**

Response: The main motive of the data audit is to check whether the practices of the organization are in compliance with the proposed policy. The committee has agreed on the evaluation of security practiced by the organization as one more aspect.

4. **Should data audits be undertaken internally by the data controller, a third party (external person/agency), or by a data protection authority?**

Response: This has to be decided by the data protection authority

5. **Should independent external auditors be registered / empanelled with a data protection authority to maintain oversight of their independence?**

Response: Yes the external auditors need to be registered with the data protection authority.

6. **What should be the qualifications of such external persons/agencies carrying out data audits?**

Response: The committee has agreed on having some Indian standards for specifying the minimum qualification of external persons/agencies carrying out the data audits

7. **Are there any alternative views on this?**

Data Protection Officer

1. What are your views on a data controller appointing a DPO?

Response:

2. Should it be mandatory for certain categories of data controllers to designate particular officers as DPOs for the facilitation of compliance and coordination under a data protection legal framework?

Response: For deciding whether a data controller should designate officers as DPOs, Indian standards should be set up

3. What should be the qualifications and expertise of such a DPO?

Response: Indian standards need to be set up for setting the minimum qualifications

4. What should be the functions and duties of a DPO?

Response: Since the data, that DPO has to deal with, varies from one data controller to another, the functions and duties of the DPO have to be framed based on the data in hand.

5. Are there any alternative views?

D. Data Protection Authority

1. What are your views on the above?

2. Is a separate, independent data protection authority required to ensure compliance with data protection laws in India?

Response: YES

3. Is there a possibility of conferring the function and power of enforcement of a data protection law on an existing body such as the Central Information Commission set up under the RTI Act?

Response: No, A separate body needs to be created.

4. What should be the composition of a data protection authority, especially given the fact that a data protection law may also extend to public authorities/government? What should be the qualifications of such members?

Response: Should include multidisciplinary knowledge (techno - legal and experience in handling National Security issues is a must)

5. What is the estimated capacity of members and officials of a data protection authority in order to fulfil its functions? What is the methodology of such estimation?

Response: At the state level depending upon the no. of districts, cities, etc

6. How should the members of the authority be appointed? If a selection committee is constituted, who should its members be?

Response: By notification of the Central/State Government with due advertisements. Selection Committee panel must consist of members from techno - legal and the ones having adequate experience in handling National Security matters.

7. Considering that a single, centralised data protection authority may soon be over-burdened by the sheer quantum of requests/ complaints it may receive, should additional state level data protection authorities be set up? What would their jurisdiction be? What should be the constitution of such state level authorities?

Response: YES. Techno - legal and the ones having adequate experience in handling National Security matters.

8. How can the independence of the members of a data protection authority be ensured?

Response: At the state level, they should have a status of a High Court Judge and at the Central level, they should have status of a Supreme Court Judge.

9. Can the data protection authority retain a proportion of the income from penalties/fines?

Response: NO

10. What should be the functions, duties and powers of a data protection authority?

Response: PI refer to response for Q 12

11. With respect to standard-setting, who will set such standards? Will it be the data protection authority, in consultation with other entities, or should different sets of standards be set by different entities? Specifically, in this regard, what will be the interrelationship between the data protection authority and the government, if any?

Response: This may include the power to: (a) issue codes of conduct/practice; (b) lay down standards for security safeguards; (c) lay down standards for data protection impact assessment; and (d) lay down standards for registration for data controllers as may be required and maintain a database in this regard. Some of these standards relate to data protection issues, e.g., standards for data protection impact assessments; others such as standards for security safeguards are not *per se* related to data protection. The role of the central government in relation to setting of standards for the latter and such analogous categories and organisational measures should be ensured.

12. Are there any alternative views other than the ones mentioned above?

Response:

- A separate and independent data protection authority may be set up in India for enforcement of a data protection legal framework. State level hierarchies must be defined for data protection authority.
- There are three broad categories of functions, powers and duties which may be performed by a data protection authority: monitoring, enforcement and investigation; standard-setting; and awareness generation.
 - (i) **Monitoring, enforcement and investigation:** This may include the power to (a) ensure compliance and enforcement with the provisions of a data protection law; (b) conduct inspection, investigations and collect documents as may be required; (c) adjudicate disputes arising between individuals and data controllers; (d) monitor cross-border transfer of data; (e) monitor security breaches; (f) issue directions to all relevant entities; (g) impose civil penalties for non-compliance; and (h) issue regulations in order to facilitate the enforcement of data protection principles and other ancillary matters relating to data protection.
 - (ii) **Awareness generation:** This may include: (a) the ability to conduct research and promote public awareness of data protection; and (b) the power to educate public and private entities.

- (iii) **Standard setting:** This may include the power to: (a) issue codes of conduct/practice; (b) lay down standards for security safeguards; (c) lay down standards for data protection impact assessment; and (d) lay down standards for registration for data controllers as may be required and maintain a database in this regard. Some of these standards relate to data protection issues, e.g., standards for data protection impact assessments; others such as standards for security safeguards are not *per se* related to data protection. The role of the central government in relation to setting of standards for the latter and such analogous categories and organisational measures should be ensured.

Chapter 3: Adjudication Process

1. What are your views on the above?

.....

2. Should the data protection authority have the power to hear and adjudicate complaints from individuals whose data protection rights have been violated?

Response: YES

3. Where the data protection authority is given the power to adjudicate complaints from individuals, what should be the qualifications and expertise of the adjudicating officer appointed by the data protection authority to hear such matters?

Response: Tehno legal qualifications are must.

4. Should appeals from a decision of the adjudicating officer lie with an existing appellate forum, such as, the Appellate Tribunal (TDSAT)?

Response: YES

5. If not the Appellate Tribunal, then what should be the constitution of the appellate authority?

6. What are the instances where the appellate authority should be conferred with original jurisdiction? For instance, adjudication of disputes arising between two or more data controllers, or between a data controller and a group of individuals, or between two or more individuals.

Response: The role of appellate authority should be exercised in case if dispute arises between two or more data controllers.

7. How can digital mechanisms of adjudication and redressed (e.g. e-filing, video conferencing etc.) be incorporated in the proposed framework?

Response: YES, Much needed in a digital economy

8. Should the data protection authority be given the power to grant compensation to an individual?

Response: YES

9. Should there be a cap (e.g. up to Rs. 5 crores) on the amount of compensation which may be granted by the data protection authority? What should be this cap?

Response: Can be considered

10. Can an appeal from an order of the data protection authority granting compensation lie with the National Consumer Disputes Redressal Commission?

Response: NO

11. Should any claim for compensation lie with the district commissions and/or the state commissions set under the COPRA at any stage?

Response: NO

12. In cases where compensation claimed by an individual exceeds the prescribed cap, should compensation claim lie directly with the National Consumer Disputes Redressal Commission?

Response: NO

13. Should class action suits be permitted?

Response: YES

14. How can judicial capacity be assessed? Would conducting judicial impact assessments be useful in this regard?

Response: YES

15. Are there any alternative views other than the ones mentioned above?

Response: As per CIC Supreme court pattern, high court, member roles to be defined.

Given that under a data protection legal regime, government bodies and public authorities may be considered as data controllers, an adjudicating officer appointed under the IT Act, who is an officer of the government, may not be the appropriate body to adjudicate disputes which involve violation of data protection obligations by such government bodies and public authorities.

It follows that an individual whose data protection rights have been violated may, at the outset, first approach the data controller or a specific grievance redressal officer of the data controller identified in this regard.

Where the data controller fails to resolve the complaint of the individual in a satisfactory and expeditious manner, the individual may be given the right to file a complaint with the data protection authority.

The data protection authority may be conferred with the power to appoint an adjudicating officer who may have the requisite qualifications and expertise to inquire into the facts of the complaint and adjudicate accordingly.

Chapter 4: Remedies

A. Penalties

In the context of a data protection law, civil penalties may be calculated in a manner so as to ensure that the quantum of civil penalty imposed not only acts as a sanction but also acts as a deterrence to data controllers, which have violated their obligations under a data protection law. Further, there may be three models (or a combination thereof) possible for the calculation of civil penalties, which are as follows:

(i) Per day basis; (ii) Discretion of the adjudicating body subject to a fixed upper limit; (iii) Discretion of adjudicating body subject to an upper limit linked to a variable parameter (such as a percentage of the total worldwide turnover of the preceding financial year of the defaulting data controller).

1. What are your views on the above?

Response: Penalty that may be imposed on a data controller or data processor based on the criteria that a supervisory authority may consider while determining the quantum of such administrative penalties. These factors include the nature, gravity and duration of the infringement taking into account the level of damage suffered; the intentional or negligent character of the infringement; any action taken by the data controller or data processor to mitigate the damage suffered by the data subjects; the degree of responsibility of the data controller or data processor taking into account the technical and organizational measures implemented by them; any relevant previous infringement by the data controller or data processor.

2. What are the different types of data protection violations for which a civil penalty may be prescribed?

Response: Its not stated explicitly in paper with examples. Data protection violations types should be classified and categorized on the basis of severity of the substantial damage or substantial distress.

3. Should the standard adopted by an adjudicating authority while determining liability of a data controller for a data protection breach be strict liability? Should strict liability of a data controller instead be stipulated only where data protection breach occurs while processing sensitive personal data?

4. In view of the above models, how should civil penalties be determined or calculated for a data protection framework?

Response: Can't suggest any specific mechanism to determine quantum of penalties except the three points stated in provisional views. It should look into various factors to calculate the penalty value as stated in answer of question 1. Or can consider the EU model factors used to govern the penalties.

5. Should civil penalties be linked to a certain percentage of the total worldwide turnover of the defaulting data controller (for the preceding financial year) or should it be a fixed upper limit prescribed under law?

Response: Civil penalties should be linked to a certain percentage of the total world wide turnover of the defaulting data controller rather than fixing upper limit.

6. Should the turnover (referred to in the above question) be the worldwide turnover (of preceding financial year) or the turnover linked to the processing activity pursuant to a data protection breach?

Response: Turnover should be the worldwide turnover linked to the processing activity.

7. Where civil penalties are proposed to be linked to a percentage of the worldwide turnover (of the preceding financial year) of the defaulting data controller, what should be the value of such percentage? Should it be prescribed under the law or should it be determined by the adjudicating authority?

Response: Cant state the percentage of the worldwide turnover. It should be determined by the adjudicating authority on case by case basis and considering all the factors such as how much damage is being done.

8. Should limit of civil penalty imposed vary for different categories of data controllers (where such data controllers are categorised based on the volume of personal data processed, high turnover due to data processing operations, or use of new technology for processing)?

Response: Yes, it should vary for different categories of data controllers including size of the company, start-up/ established, overall turnover worldwide.

9. Depending on the civil penalty model proposed to be adopted, what type of factors should be considered by an adjudicating body while determining the quantum of civil penalty to be imposed?

10. Should there be a provision for blocking market access of a defaulting data controller in case of non-payment of penalty? What would be the implications of such a measure?

Response: Yes, in case default data controller not able to pay the penalty, should have provision for blocking market access of default data controller.

11. Are there any alternative views on penalties other than the ones mentioned above?

Response: No

B. Compensation

Awarding of compensation constitutes an important remedy where an individual has incurred a loss or damage as a result of a data controller's failure to comply with the data protection principles as set out under law.

1. What is the nature, type and extent of loss or damage suffered by an individual in relation to which she may seek compensation under a data protection legal regime?

Response: Taking provisional views and EU model guidelines into the consideration we can say: an individual who has suffered any kind of loss or damage as a result of the infringement of the EU GDPR shall have the right to receive compensation from the data controller or data processor for the damage suffered.

2. What are the factors and guidelines that may be considered while calculating compensation for breach of data protection obligations?

Response: In Accordance to Provisional views, claim for compensation may be filed in accordance with the provisions set out in the previous chapter on Adjudication Process. If an individual claims a certain amount as compensation, she will be required to demonstrate how the data controller's failure to comply with the law has resulted in her incurring that amount of damage or loss.

3. What are the mitigating circumstances (in relation to the defaulting party) that may be considered while calculating compensation for breach of data protection obligations?

4. Should there be an obligation cast upon a data controller to grant compensation on its own to an individual upon detection of significant harm caused to such individual due to data protection breach by such data controller (without the individual taking recourse to the adjudicatory mechanism)? What should constitute significant harm?

Response: No there should not be any obligation cast on the data controller in that case.

4. Are there any alternative views other than the ones mentioned above?

.....NO

C. Offences

The law may treat certain actions of a data controller as an offence and impose a criminal liability. This may include instances where any person recklessly obtains or discloses, sells, offers to sell or transfers personal data to a third party without adhering to relevant principles of the data protection law, particularly without the consent of the data subject. It may be considered whether other acts should create criminal liability.

1. What are the types of acts relating to the processing of personal data which may be considered as offences for which criminal liability may be triggered?

Response: In accordance to the provisional views with little modification:: The law may treat certain actions of a data controller as an offence and impose criminal liability. This should include instances where any person recklessly obtains or discloses, sells, offers to sell or transfers personal data to a third party without adhering to relevant principles of the data protection law, particularly without the consent of the data subject.

2. What are the penalties for unauthorised sharing of personal data to be imposed on the data controller as well as on the recipient of the data?

3. What is the quantum of fines and imprisonment that may be imposed in all cases?

Response: We agree as per the provisional views “The quantum of penalty and term of imprisonment prescribed may be enhanced as compared to the provisions of the IT Act.”

4. Should a higher quantum of fine and imprisonment be prescribed where the data involved is sensitive personal data?

Response: Yes, it should define higher quantum of fine and imprisonment when data involved is sensitive personal data.

5. Who will investigate such offences?

Response: It should be decided by the Data protection authority that whom should we address for investigation.

6. Should a data protection law itself set out all relevant offences in relation to which criminal liability may be imposed on a data controller or should the extant IT Act be amended to reflect this?

Response: As it already been stated in IT act, it should be amended to reflect all the relevant offences in relation to criminal liability imposed on a data controller.

7. Are there any alternative views other than the ones mentioned above

Response: No

Summary

The deliberations of the workshop have raised many crucial issues with regard to the linkages between unfettered processing of individual data and matters of national security. We have kept in mind the individual's right to privacy, particularly the vulnerabilities of children and underprivileged class. Due consideration has also been given to digital commerce and the need to ensure that innovation and entrepreneurship in India is not disadvantaged. However, we are also conscious that economics cannot override national security. As John J. Mearsheimer points out in his book, *The Tragedy of Great Power Politics*, “(In) matters of national security, because concerns about survival are invariably at stake...they are more important than worries about prosperity.”

Some key recommendations are summarised below.

Data Localisation

Our discussions revealed the territorial limits of jurisdiction. It is extremely difficult to protect data, which resides in other countries, particularly where the data controller does not have any presence in India. U.S. courts are even asking technology companies registered in the country to provide data, which is located outside the U.S. borders. One-way suggested was to have bilateral treaties with various countries but this a protracted process.

The only solution lies in localising the sensitive data of Indian citizens within the boundaries of India. While currently the infrastructure for this may not exist, it would come up if the data controllers wish to continue to take advantage of the size of the Indian market.

The advent of IoT would exponentially increase the volume of data being generated. Any new infrastructure being created for IoT should also make arrangement for data to be stored in India.

The Cyber physical systems are collecting huge information for data analysis and doing unprecedented personal sensing and the data is freely flowing across borders without being sanitized, which can have very serious implications. Initiatives like Digital India, startup India, smart city should be planned in such a manner that a framework needs to be worked out which takes into account the peculiar development circumstances

We understand that cross-border flows of data cannot be completely stopped. However, no sensitive personal data should be permitted to go outside the country. There should be legal restrictions on transfer of data to controllers who have no presence in India.

Sensitive Data

The White Paper has given a comprehensive definition of sensitive personal data. However, this definition is based on the sensitivity of the information from an individual perspective and not from national security. As an example, should the data of intelligence officials or military officers, stored in one place, be considered sensitive, even though it has only basic personal data? There could be many such cases and therefore there is a need to classify such data also as sensitive.

Data Processing

Individuals are generating vast amount of data each time they carry out any electronic activity. This information is automatically stored by data controllers. It is difficult to keep a check on this activity but the processing of data must be for a specific and limited purpose.

With aggregation of data and advanced algorithms for processing, it is possible to build up an accurate profile of an individual, which reveals many traits of his character. This knowledge could be used to influence opinions or even stir up trouble and strife between communities. Such analytical profiling can be checked if the processing of data is strictly controlled. Sale of personal data to data brokers must also meet stringent legal criteria.

Individual Rights

By having greater control and visibility over their data, individual can indirectly contribute towards national security. The White Paper has correctly identified Individual Participation Rights like confirmation, access to data, right to object and the right to be forgotten. These will strengthen individual privacy.

In addition to these it is important that an individual is aware of all the data controllers who have access to his personal data. This is important because data is regularly being shared between various entities without the individual coming to know. This will also put some check on the practice of routinely asking for personal data even when not essential.

Economic Impact

A reading of the White Paper shows that there is some apprehension that a stringent data law could have an adverse financial impact. In our discussions, we did not find any fact that could support this apprehension. In fact, in the long term, data localisation and development of Indian Standards will help the indigenous industry.

Foreign Investment firms will need to set up their data centres within the territory of India and this will mean newer opportunities for the Indian IT skilled professionals. The government will be motivated to setup an in-house IT industry and start-up sector focusing on development of Indigenous technology. With Data Localisation a lot of personal data of the Indian Residents will return to Indian borders. There will be a large scope for domestic data transformation projects. Many MNCs will be compelled to start with migration projects, which in turn will fetch a lot of capital.

Conclusion

The need for a data protection law was triggered by the debate on individual privacy. However, the importance of this data for national security must not be overlooked. It is for this purpose that the workshop held at PEC focused on the how the proposed law must also strengthen India's national security.