White paper on data protection: Summary and Questions

Rachit Garg
Department of Computer Science and Engineering
Indian Institute of Technology Madras

September 8, 2018

Contents

1 Disclaimer

The views contained in the report are the personal views of the student and do not endorse or reflect the views of the institute.

2 Introduction

The vision of our country to be a digital economy and perform business on a global electronic scale necessitates the creation of laws that secure the data of individuals. A firm legal framework for data protection is the foundation on which data-driven innovation and entrepreneurship can flourish in India. Fostering such innovation and entrepreneurship is essential if India is to lead its citizens and the world into a digital future committed to empowerment, experiment, and equal access.

It is believed that by 2020, the global volume of digital data we create is expected to reach 44 zettabytes (14). Enterprises around the world have realized the value of these databases and are continually investing in technology for its proper mining and use. There are algorithms being developed to find patterns within data to decide on activities which can be beneficial to society. There are also a lot of opportunities for businesses to improve and capture a larger share of the market using such approaches. An example of this was the Netflix data challenge. The original intention of the competition was to generate an algorithm that can better be suited for their business and beneficial to the users. But the anonymized Netflix data could be easily combined with other data sets such as timestamps with public information from the Internet Movie Database(IMDb) to de-anonymize the original data set and reveal personal movie choices (30). Such instances warn us about this fast-moving field and warrant us to be cautious as well.

India presently does not have any express legislation governing data protection or privacy. The relevant laws in India dealing with data protection are the Information Technology Act, 2000 and the (Indian) Contract Act, 1872. Under section 43A of the Indian Information Technology Act,2000, if an organization is negligent in maintaining security practices or uses them for wrongful gain may be held liable to pay damages to the person so affected. These laws are not explicit enough in their statements. The specificities about the actual pay damages, the definition of personal, sensitive information or the technicalities of what is constituted as negligence are presently unclear in the law. The issue is that either the details are not explicitly stated or they overlook some key details which are ever-growing as new data-driven technologies hit the market.

Technology convenience and benefits are something that even the courts have realized. The Delhi high court recently accepted a WhatsApp notification as receipt proof (25). After a long battle, the Supreme court in its verdict in Puttaswamy acknowledged the need of data privacy laws. The Supreme Court in Puttaswamy (29) overruled its previous judgments of M.P. Sharma v.Satish Chandra (M.P. Sharma) (1) and Kharak Singh v. State of Uttar Pradesh (Kharak Singh) (2) and held that Article 21 of the Constitution of India is the repository of residuary personal rights and it recognized the right to privacy. But even with this precedent, without a proper law, the courts are regularly being presented with cases and issues (16).

These incidents call for an urgent need for these laws. Laws must be made keeping in mind the views and beliefs of Indians and must work well with an increasingly interconnected world. In 1989, researchers from Arizona State University partnered with the Havasupai Tribe, a community with high rates of Type II Diabetes, to study links between genes and diabetes risk. The researchers were unsuccessful in finding concrete patterns but they used the same data for other studies such as schizophrenia, migration, and inbreeding. These topics are considered taboo by the tribe (11; 23). Such incidents should remind us of the fact that we need to take into account a communities' beliefs when processing their private data. We need to be aware and cognizant of the comparative and international practices.

Even with this urgent need, we must be careful of the laws that are created and do not make decisions in haste. In the recent past, the Indian government has not been careful with the privacy of user data. The Aadhaar project, which is one of the worlds largest identity projects, has had serious privacy concerns (15). The Aadhaar Act enables the Government to collect identity information from citizens (3), including their biometrics, issue a unique identification number or an Aadhaar Number on the basis of such biometric information (4), and thereafter provide targeted delivery of subsidies, benefits, and services to them (5). The project received a lot of criticism from social commentators and civil society activists (27; 19; 20) due to the way the privacy was seen and implemented. Although there were a few suggestions (13) and recommendations from Shah (The Planning Commission: Government of India, 2011), Sinha (Lok Sabha Secretariat: New Delhi, 2012) committees (12) and the computer science community (33), the present security of the Aadhaar project continues to be under scrutiny with serious concerns. (32).

Data protection norms for personal information collected under the Aadhaar Act are also found in the Aadhaar (Data Security) Regulations, 2016 (Aadhaar Security Regulations). The Aadhaar Security Regulations impose an obligation on the UIDAI to have a security policy which sets out the technical and organizational measures which will be adopted by it to keep information secure. But the present developments suggest that these policies still might not be enough (33), and we need to be really careful and keep in mind the implementation aspects of such a project along with the laws.

3 Scope And Exemptions

3.1 Territorial and Personal Scope

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

  For territorial scope, the primary test for applicability of law should be processing of

personal information which takes place in the territory of India. This should cover Indian entities and non-Indian entities that do not have a presence in India but process the data associated with the Indian population.
Extraterritorial application of data protection must ensure that the data associated with any Indian entity is adequately protected and must observe the enforceability of such a law. Recently, a five-judge constitution bench headed by Chief Justice Dipak Misra did not pass an order but directed WhatsApp to file an affidavit giving details of what user data was shared with third parties and other entities within four weeks (16). In this particular case, on 25 August 2016, the users were sent a notification by WhatsApp asking them to accept the changes in terms and conditions. This allowed them to share this data with Facebook for commercial use. This draws attention to the fact that these notifications should not be left to the consent of users who fall into the trap of consent fatigue and multiplicity of notices.
India is a very diverse nation with endless varieties of physical features and cultural patterns. We cannot expect non-territorial laws to keep in mind the unique beliefs of different cultures. Particularly, we would not want our sensitive personal data to be used to challenge beliefs, as it happened in the case of the people of Havasupai tribe(see above 2) (11; 23)

- To what extent should the law be applicable outside the territory of India in cases where data of Indian residents are processed by entities who do not have any presence in India?
  There should be strict regulation of data in cases where sensitive data of Indian residents are involved. For data which does not come under the category of sensitive data, this becomes more a question of cross-border data flow or imposing laws that regulate usage of data within foreign nations.
  In the former scenario of cross-border data flow the two approaches mentioned are the adequacy test and the comparable level of protection for personal data which will be determined by a data protection authority. This requires a strong, well-formed and updated data protection authority. The latter scenario is less feasible as it has problems with enforceability; it also makes for the entity doing business to be caught among laws from various places which can lead to contradictions and legal hassles. Hence we must be careful in the distinction, it may be reasonable to ask a foreign company to abide by a country's abuse-prevention rules (rules that prevent unauthorized use of personal data), but it is less feasible to impose on the company the duty of designating a Data Protection Officer. One such solution is to use a hybrid multi-layered approach as mentioned in (34).

- While providing such protection, what kind of link or parameters or business activities should be considered?
  Covering of cases where processing wholly or partly happens in India, irrespective of the status of the entity, is an approach which does not cover the full application of

the law. The data of Indian people can come under a scenario where the processing is completely done outside. An Indian user might be accessing a site or company based in the USA and can get into conflicts with them. Regulating entities which offer goods or services in India even though they may not have a presence in India (modeled on the EU GDPR) seems to be the correct view here. Regulation should be subjective so that it does not demote further business opportunities.

- 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?
  In such a case a sensible approach is to adopt the penalties the EU GDPR prescribes based on global turnover (6). Further, a failure to pay fines or to comply with any other sanctions imposed by the law could be linked to an order restricting market access (28).

3.2 Other issues of scope

- What are your views on the issues relating to the applicability of a data protection law in India in relation to:
  - natural/juristic person
  - public and private sector
  - retrospective application

  of such a law?
  The laws should be applied to a natural person. For juristic individuals, a separate analysis needs to be done. This can be considered in future versions of the law.
  Public and private sectors should have a common law. The Kharak Singh vs State of Uttar Pradesh (1962) case (2) brought into light the same dilemma. Public institutions should only be granted exemptions under very specific instances.
  Retrospective application of the law is extremely necessary. However, there needs to be special care taken to define what measures can be taken on these instances. These measures need to be consistent enough so that their application is possible and the time taken to implement those measures is also taken into account.

- Should the law seek to protect data relating to juristic persons in addition to protecting personal data relating to individuals?
  The law could regulate personal data of natural persons alone for the time being. It is coherent with most data protection legislations around the world. If it was chosen to apply these, it creates issues. It may definitely provide better protection to companies for their confidential business data. It may also, however, create conflict between contractual arrangements like the confidentiality agreements and the law, similar to those seen with licensing agreements and copyright law.

- Should the law be applied to government/public and private entities processing data equally? If not, should there be a separate law to regulate government/public entities collecting data?
  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. The Right to Privacy should be a fundamental right and only under very specific instances which are listed down explicitly should the public sector be exempted.

- 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?
  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.
  A method needs to be devised to deal with such past illegal collections of data. We can see an example in the Facebook case where a decision must be made on what happens to the data already disclosed to Facebook (16).

- 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?
  Yes, we must give adequate time for the industry to adapt to these regulations. The law that is decided will have a lot of facets and can be complicated to comprehend. Since there might be components in the law that need to be implemented securely to the end user, the industry will need time to meet the required regulations.

3.3 Definition of Personal Data

- For the purpose of a data protection law, should the term personal data or personal information be used?
  Adopt one term, personal data as in the EU GDPR or personal information as in Australia, Canada or South Africa.

- 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?
  The idea to qualify identifiable data as personal data seems to be the correct approach. But as the technology is expanding, social media is exploding and innovative ideas are coming up, it seems difficult as to what may be identifiable. There might be patterns in the random data points which might be learned. An example where this confusion can clearly be seen is the Netflix data challenge (30). The data was

anonymized by the problem setters but it was realized later that the data could "identify" the people when combined with a public IMDb dataset. The most challenging question here is to adequately define what will be included in the data so that privacy is ensured.
It should include any kind of facts, opinions or assessments keeping in mind the accuracy of the statements. Anything that can either lead to defamation, identification or breach of a person's belief system. Defaming people on social media by stating incorrect facts, opinions and assessments can lead to a questionable reputation in the community. Modified photos that scandalize persons or businesses are clear defamation violation and are quite popular on social media. It is common for modified photos or video to go 'viral'. In such a case, the accuracy of the statements made should be taken into account.
Selling of opinions and facts by companies to other organizations so that targeted ad campaigns can be made and public opinion be modeled is one of the new weapons of the digital age. The algorithm used in the Facebook data breach trawled through personal data for information on sexual orientation, race, gender and even intelligence and childhood trauma. It also claimed that it can influence voters by targeting them with personalized ads (18). Another case where a communities belief system was overlooked was the case of the Havasupai tribe(See above 2) (11; 23).

- Should anonymized or pseudonymized data be outside the purview of personal data? Should the law recommend either anonymization or pseudonymization, for instance as the EU GDPR does?
  From a cryptographic standpoint, simply removing the identity as in anonymization is not enough for disguising identities. A study has shown that its possible to personally identify 87 percent of the U.S. population based on just three data points: five-digit ZIP code, gender, and date-of-birth (35). Thus, what constitutes as identifiable is difficult to answer and this places huge concerns on data. Cryptographic protocols that can securely de-anonymize datasets and allow computation of different functions on any kind of datasets are far from being efficient today(Functional Encryption (17) and Fully Homomorphic Encryption (22)). Advances in this field will really open new possibilities and the government should keep an eye on these.
  Anonymization is not enough as seen in the scenario of Netflix users (30) and pseudonymization is an even weaker outlook towards things. The EU GPDR places a greater emphasis on anonymization and introduces notions of pseudonymization in many scenarios (7). Our laws should also de-segment the cases and mention specifically which approach should be taken and when. Special care needs to be taken on the techniques that will be used for these purposes and that they are implemented by experts in the field only.

3.4 Definition of Sensitive Personal Data

- Should the law define a set of information as sensitive data? If yes, what category of data should be included in it? Eg. Financial Information / Health Information / Caste / Religion / Sexual Orientation. Should any other category be included?
  Financial Information, Health Information, Sexual Orientation should be included in sensitive personal data. Categories such as caste and religion are also sensitive and can be a cause for discrimination in our society. But we need to be careful in the formulation of the law as to what will categorize as sensitive information. A person's name can, in many cases, be related to their caste or religion, and shouldn't be included as sensitive but explicitly mentioning their caste or religion should be. Genetic data and biometric data should also be included in these categories as these form an integral part of our identity. Also with the Aadhaar Act and phone authentication functions, there is a huge importance placed on a person's biometric data. An increasing amount of sensitive biometric data is also being collected, whether through fingerprints, face patterns for authentication, DNA collection, or fitness apps tracking traits.
  Data regarding the physical location of a person is also a category which should be added. It is extremely sensitive information about a person's whereabouts. Travel apps or taxi cab apps should not make this data public or sell these to third parties. There was one such incident where a journalist was threatened by Uber executives using privately collected user data (24).
  Under financial information, the law needs to be clear as to what details should be included. The transaction histories of a person, their purchases and bill payments presently can easily be disclosed to third parties.

3.5 Definitions of Processing

- 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?
  I believe it should inclusively cover all possible operations. Exclusively mentioning might miss operations that are innovated later. Also, this gives the law a broader coverage to regulate on.

- 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?
  If data is collected manually, only filing systems should be covered as the risk of profiling is lower in other cases. This is the feasible way to go about things. The option of including all personal data processed, however, it may be processed, is infeasible in terms of upholding the law as we as individuals are always manually

processing data. Limiting to digital or automated records is against the retrospective application and limits the applicability of the law in many scenarios in India where digitization is not the main method of data collation.

3.6 Definition of Data Controller and Processor

- Should the law only define 'data controller' or should it additionally define 'data processor'?
  Use the two concepts of 'data controller' and 'data processor' (an entity that receives information) to distribute primary and secondary responsibility for privacy, because in many cases data is outsourced to entities.

- How should responsibility among different entities involved in the processing of data be distributed?
  There should be a clear bifurcation of roles and associated expectations from various entities. The expectations might not be explicitly clarified contrary to the case of EU GDPR as the compliance costs on data processors can be high (21). Concerns relating to the enforceability of contracts and enforcement capabilities in India must also be taken into account. The law can identify different entities and relate them to broad expectations and not be stringent in its application.

3.7 Exemptions

- What are your views on including research/historical/statistical purpose as an exemption?
  The kind of research that we can conduct as an exemption needs to keep in mind the sentiments of the data owner. In the late 1980s, researchers violated the sentiments of the Havasupai tribe. They claimed to use this data for diabetes research but instead used it for unrelated topics and studies about migration, inbreeding, schizophrenia. These topics are considered taboo by the Tribe and hence were an ethical violation of the feelings of an entire community. (See above 2). Also, the usage of this data for commercial purposes needs to be taken care of. Today India's Aadhaar act has led to the collection of one of the largest databases in the country. Protected sharing of this data can help immensely in research/historical/statistical purposes.
  I strongly believe that exemptions only through proper approvals should take place and we need to keep in mind the different beliefs and the consent of the people. As India is a diverse country, these beliefs are often subjective and hence the exemptions should be seen on a case to case basis.

3.8 Cross Border Flow of Data

- 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?
  Yes, there should be laws in place for facilitating cross-border transfer of data. Such cross-border flow of data can be seen in the case of BPOs. A global data flow can play an important role in promoting trade, research, and development in the country. Although we should be careful to not send the sensitive data across the border. The adequacy standard seems a good test for deciding the countries where the transfer of data can occur too. We can decide on countries which have good implementations of data privacy laws and trust their legal system to uphold the rights of Indians. If we create more stringent laws then enforcing it on foreign territory might not be easy.

- Should certain types of sensitive personal information be prohibited from being transferred outside India even if it fulfills the test for transfer?
  Yes, the sensitive personal information should be prohibited from being transferred outside the country. This includes financial information, health information, genetic build up and all the categories which come under the sensitive data umbrella. These are private data and due to the complications that arise with the enforcement of laws across boundaries. One such instance where problems can clearly be seen is the case of Microsoft against the US government. Microsoft refused to provide the details of certain emails, basing their legal argument on the fact that the data requested was stored in servers outside US (26).

3.9 Data Localization

- Should there be a data localization requirement for the storage of personal data within the jurisdiction of India? If yes, what should be the scope of the localization mandate? Should it include all personal information or only sensitive personal information?
  In my view, it must include all the data generated by users in the digital domain. Localised storage and processing of sensitive data is mandatory as currently there isn't a unified framework for data protection laws throughout the world. This also prevents foreign surveillance and easier law enforcement that will take into account the varied beliefs of the people of this country (26).
  This, however, can lead to increased local surveillance. Large-scale government surveillance should not be allowed on this data, only under specific assumptions should the government be given controlled access to the data.

- If the data protection law calls for localization, what would be the impact on industry and other sectors?

One impact of data localization on industry and other sectors is that regulations hinder the new and upcoming startups. Local storage and processing means that the low-cost benefits of cloud computing and other data storage services cannot be used, hence the cost of performing efficiently and maintaining themselves now lies on the head of the small startups. This also prevents companies from around the world in investing in the data of our nation. In the future, if big data algorithms turn extremely successful, China being a closed market would mean that India would be the natural destination for investments to gather data. Here, we must lay down the law carefully so that we do not slow development in hope for stringent laws.

Even in the light of above advantages, local storage will allow for more stern control by the regulator. All data should be stored and processed on systems located within India. We should not compromise security in hope for increased investment.

4 Grounds of Processing, Obligation on Entities and Individual Rights

4.1 Consent

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

  An individual's consent should be valid only if an individual could reasonably expect to understand the nature, purpose, and consequences of the collection, use or disclosure of the personal information to which she has consented.

  Consent should be a primary ground for processing. User consent is a must for any use of their data. As the technology is expanding at an accelerated pace, we might not be able to foresee what processing might mean in the future. Individuals may be able to foresee an immediate harm caused by misuse of their personal information, however, it is highly unlikely that they will be able to predict future uses of their information, which takes place after combining it with other data sets. Also, there are many users that fall into the trap of consent fatigue and multiplicity of notices. Hence in general consent should be a necessary but not sufficient ground for processing. Reason must be stated clearly as to what this data is to be used for. For any alteration or additional use, new consent must be taken from the user.

- 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?

  Consent that is given should be clear in its articulation, revocable and auditable.

  It seems logical to assume implicit consent in cases where the data is not sensitive and require for explicit consent when processing personal data. All transactions may not warrant the same standards of consent. Therefore, there is a need to explore

and accommodate standards of consent within the data protection law and align it with different types of information. These details should also be evolved and updated through the legislation at regular intervals.
These requirements might be onerous for non-sensitive data, but for sensitive data these details are mandatory.

- How can consent fatigue and multiplicity of notices be avoided? Are there any legal or technology-driven solutions to this?
  A service might share a video indicating what kind of data will be used by the service, although mandating such a video in this law is not feasible. It is something that the industry should thrive towards as they move forward. Other technological solutions might include designing a parser that can parse through the more relative parts of the documents, and mentions alternate options for the legal terms.
  In terms of legal driven solutions, there can be a committee that looks into these notices and regulates these so that they are not as confusing to the end user. These notices are extremely long and the jargon used in these cases is often very complicated. The data controller who processes the data must get these notices passed by this community.

- Would, having very stringent conditions for obtaining valid consent be detrimental to day-to-day business activities? How can this be avoided?
  Obtaining valid consents do exist in many of the current businesses settings. There might be some businesses that will get affected by these laws, but soon these will become a standard.

4.2 Child's Consent

- What are your views regarding the protection of a child's personal data?
  An individual's consent should be valid only if an individual could reasonably expect to understand the nature, purpose, and consequences of the collection, use or disclosure of the personal information to which she has consented. Keeping this view in mind, distinct provisions could be carved out within the data protection law which prohibit the processing of children's personal data for potentially harmful purposes, such as profiling, marketing, and tracking.

- 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?
  No, I believe this to be an extremely strict notion for students to not use the internet. This also is against digital learning.

- 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?

The entity which collects the information. The test though should carefully be set in place by the data protection authority.

- How can the requirement for parental consent be operationalized in practice? What are the safeguards which would be required?
  Parental consent needs to be secure. It can be linked to the parent's identity using KYC and OTPs. Another way in which a child's consent can be obtained is through zero-knowledge proofs which might be able to verify their age without revealing explicit information about their identity. These solutions can be combined to ensure informed consent.

4.3 Storage Limitation and Data Quality

- What are your views on the principles of storage limitation and data quality?
  Storage limitation in my view is necessary to prevent storing mass data about an individual. Presently there are no checks in place, this can lead to enterprises or governments storing large chunks of data about individuals. With a big data revolution and newer algorithms, there is no say at what stage storing excessive data might make a person identifiable. In the case of Cambridge Analytica, we saw how this lead to influence an individuals choice of voting and decide on their sexual orientations (18). All data processers must be allowed to share, or collude this data with anyone or any external party for any business purpose.

- On whom should the primary onus of ensuring the accuracy of data lie especially when consent is the basis of collection?
  The onus should be over to the data controller, and the data owner should have the right to access and rectify, modify its data.

- How long should an organization be permitted to store personal data? What happens upon completion of such time period?
  Any organization must state upfront the duration for which user data is being used/ stored, after that the data must be completely erased for the benefit and security of user. Even during use, the data should be anonymized under the constraint of informed consent from the user. In such a case the user must be aware of the exact data fields which will be removed and which part of their data will be remembered.

4.4 Individual Participation Rights - 1

- Should there be a fee imposed on exercising the right to access and rectify ones personal data?
  This depends on the usage of the personal data. If the personal data is a consequence of a fundamental right and a necessary part of an individuals identity such as the details in Aadhaar, changing them should be free of cost. On the other hand, in

the commercial sector, this fees can be asked and should be under regulation so that companies don't deny the users by asking for outrageous amounts. For small startups, there can be provisions in the government where the government promotes usage of services that will be suitable for the right to access and hence allow startups to participate in ensuring such facilities and thus incorporating such functions in the industry.

- 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 to court to get an order to rectify, block, erase or destroy inaccurate data as is the case with the UK?
  Yes, it should include clauses which court orders can remove. A person should have the right to rectify their data, this includes right to edit, replace, or erase their data. Simply correcting out of date data will not be a sufficient application of the law. To achieve this, there must be a system to recognise a request for rectification and an understanding of the application of this right. There must in accordance be procedures or policies that ensure that proper response to such requests are ensured. This should be coupled with a receipt ensuring that the appropriate changes were made or valid/justifiable explanations for refusal of such a request.

- 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?
  I dont think this is presently feasible. If India were to encourage moving towards such a functionality. Services that allow access to large-scale data which can be centrally (usable by the data controller), dynamically(subject to changes), and securely(data should be secure from malicious users) should be promoted in India.

4.5 Individual Participation Rights - 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?
  The right to data portability is extremely important and shouldn't be restricted. The same is true for the right to restrict processing, however, for both, there might be some explicit exceptions stated and a time period be provided so that the law can be upheld properly.

- Should there be a prohibition on evaluative decisions taken on the basis of automated decisions?
  There should be a right to object to automated decisions as is the case with the UK.

4.6 Individual Participation Rights - 3: Right to be forgotten

- Does a right to be forgotten, add any additional protection to data subjects not already available in other individual participation rights?
  Yes, this right is an extremely important addition and it does indeed offer additional protection to subjects. It is also worth noting that this functionality has not been noted anywhere else in the white paper document, and a right such as this is essential in order to ensure privacy.

- Are there any alternative views on this?
  I believe it is extremely necessary to formally recognize the ways in which the data is forgotten. Whether it can still be accessed by anyone. Like in the verdict of Google Spain the data can be simply accessed by opening a VPN connection (10). Also with many Wayback Machine sites available which contain the information about the internet at a time in the past. To accurately define forgotten will be important (8).

5 Conclusion

The white paper document addresses various important issues and does a good job of categorizing approaches and discussing solutions. One area in which the white paper document completely overlooks is the view of the laws with respect to cryptography. Encryption and other cryptographic protocols form an extremely important facet to computer security. The document overlooks and doesn't ask questions about what cryptographic assumptions should be considered secure under the law. If we were to cryptographically secure the data, then, will we be able to send it across borders? If yes, which protocols are the ones on which we can concentrate, for effective communication in India? If there are such protocols that exist in the future (blockchain technology is one interesting primitive that seems to be a good secure alternative for keeping databases secure and usage more transparent), should they be made mandatory in law for the welfare of the citizens? Even Europe's GDPR doesn't define these notions explicitly (9). Their idea of anonymizing or pseudonymizing is very different from cryptographic techniques which rely on well worked out security proofs and well studied mathematical assumptions. These technologies are used widely in financial banking transactions, healthcare to general surfing over the internet. The government should look at these modern techniques and make provisions for these in the law.

References

[1] M.P. Sharma v. Satish Chandra, (1954) SCR 1077.

[2] Kharak Singh v. State of Uttar Pradesh, (1964) 1 SCR 332.

[3] Section 30, Aadhaar Act.

[4] Section 3, Aadhaar Act.

[5] Section 7, Aadhaar Act.

[6] Article 83, EU GDPR.

[7] https://iapp.org/media/pdf/resource_center/PA_WP2-Anonymous-pseudonymous-comparison.pdf.

[8] http://archive.org/web/. Online; accessed 18 June 2018.

[9] Gdpr encryption: what you should know and what you do not know. https://www.i-scoop.eu/gdpr-encryption/. Online; accessed 18 June 2018.

[10] Google spain sl v. agencia espaola de proteccin de datos. https://globalfreedomofexpression.columbia.edu/cases/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos-aepd/. Online; accessed 18 June 2018.

[11] Havasupai tribe and the lawsuit settlement aftermath. http://genetics.ncai.org/case-study/havasupai-Tribe.cfm. Online; accessed 18 June 2018.

[12] Report of the group of experts on privacy. http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf. Online; accessed 18 June 2018.

[13] List of recommendations on the aadhaar bill, 2016 - letter submitted to the members of parliament. https://cis-india.org/internet-governance/blog/list-of-recommendations-on-the-aadhaar-bill-2016, 2016. Online; accessed 18 June 2018.

[14] The digital universe of opportunities: Rich data and the increasing values of the internet of things. https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm, April 2014. Online; accessed 18 June 2018.

[15] Aadhar bill passed in lok sabha, opposition fears surveillance. https://indianexpress.com/article/india/india-news-india/aadhar-card-uid-bill-lok-sabha-arun-jaitley/, March 2016. Online; accessed 18 June 2018.

[16] Supreme court tells whatsapp to give details of user data it shared with third parties. https://www.livemint.com/Industry/4ZHBBToChW2T6JMThhjR9L/SC-tells-WhatsApp-to-give-details-of-user-data-it-shared-wit.html, September 2017. Online; accessed 18 June 2018.

[17] Boneh, D., Sahai, A., and Waters, B. Functional encryption: Definitions and challenges. In *TCC* (2011).

[18] Cadwalladr, C., and Graham-Harrison, E. How cambridge analytica turned facebook likes into a lucrative political tool. https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm, March 2018. Online; accessed 18 June 2018.

[19] Chinmayi, A. Privacy is a fundamental right. http://www.thehindu.com/opinion/lead/lead-article-on-aadhaar-bill-by-chinmayi-arun-privacy-is-a-fundamental-right/article8366413.ece, September 2016. Online; accessed 18 June 2018.

[20] Drze, J. The aadhaar coup. http://www.thehindu.com/opinion/lead/jean-dreze-on-aadhaar-mass-surveillance-data-collection/article8352912.ece, September 2016. Online; accessed 18 June 2018.

[21] Gabel, D. D., and Hickman, T. Chapter 11: Obligations of processors unlocking the eu general data protection regulation. https://www.whitecase.com/publications/article/chapter-11-obligations-processors-unlocking-eu-general-data-protection, July 2016. Online; accessed 18 June 2018.

[22] Gentry, C. Fully homomorphic encryption using ideal lattices. In *STOC* (2009).

[23] Harmon, A. Indian tribe wins fight to limit research of its dna. https://www.nytimes.com/2010/04/22/us/22dna.html?pagewanted=all&_r=1&, April 2010. Online; accessed 18 June 2018.

[24] Kastrenakes, J. Uber executive casually threatens journalist with smear campaign. https://www.theverge.com/2014/11/18/7240215/uber-exec-casually-threatens-sarah-lacy-with-smear-campaign, November 2014. Online; accessed 18 June 2018.

[25] Manral, M. S. Court accepts whatsapp blue double-tick as receipt proof. https://indianexpress.com/article/india/court-accepts-whatsapp-blue-double-tick-as-receipt-proof-summon-delhi-hc-4661278/, May 2017. Online; accessed 18 June 2018.

[26] McCarthy, K. Us govt can't stop microsoft taking its irish email seizure fight to the supreme court. https://www.theregister.co.uk/2017/01/24/us_government_microsoft_email_seizure_appeal/, January 2017. Online; accessed 18 June 2018.

[27] Mehta, P. B. Privacy after aadhaar. http://indianexpress.com/article/opinion/columns/privacy-after-aadhaar-money-bill-rajya-sabha-upa/, September 2016. Online; accessed 18 June 2018.

[28] Rahmansyah, D., and Tahir, S. Data protection in indonesia: overview. https://content.next.westlaw.com/Document/Ic7ba28fe5f0811e498db8b09b4f043e0/View/FullText.html?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1, October 2017. Online; accessed 18 June 2018.

[29] Reddy, J. Right to privacy: Sc's verdict on ks puttaswamy case is landmark, but raises five interesting law and policy issues. https://www.firstpost.com/india/right-to-privacy-scs-verdict-on-ks-puttaswamy-case-is-landmark-but-may-raise-few-law-and-policy-issues-3988913.html, August 2017. Online; accessed 18 June 2018.

[30] Schneier, B. Why 'anonymous' data sometimes isn't. https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/, December 2017. Online; accessed 18 June 2018.

[31] Sen, S. Paytm offers unsecured loans to small businesses, mobikwik to follow suit. https://www.hindustantimes.com/business-news/paytm-offers-unsecured-loans-to-small-businesses-mobikwik-to-follow-suit/story-SwTyKWpVxVGfTwaqoKku2K.html, July 2016. Online; accessed 18 June 2018.

[32] Sethi, A., and Bansal, S. Aadhaar gets new security features, but this is why your data still may not be safe. https://www.hindustantimes.com/india-news/aadhaar-gets-new-security-features-but-this-is-why-your-data-still-may-not-be-safe/story-RoZJAOUXtWZREr4V4M5TvK.html, July 2017. Online; accessed 18 June 2018.

[33] Shweta Agrawal, Subhashis Banerjee, S. S. Privacy and security of aadhaar: A computer science perspective. Economic and Political Weekly, September 2016.

[34] Svantesson, D. A "layered approach" to the extraterritoriality of data privacy laws.

[35] Sweeney, L. Simple demographics often identify people uniquely.