RESPONSES TO THE WHITE PAPER OF THE COMMITTEE OF EXPERTS ON DATA PROTECTION FRAMEWORK FOR INDIA

A LENS ON HEALTH DATA

HARVARDFXB
CENTER FOR HEALTH AND HUMAN RIGHTS

CO-CHAIRS

Satchit Balsari, MD, MPH
Faculty, Emergency Medicine, Harvard Medical School
Harvard TH Chan School of Public Health

Professor Jacqueline Bhabha
Professor of the Practice of Health and Human Rights
Director of Research, Harvard FXB Center for Health and Human Rights

EDITOR

Kundhavi Suresh Kumar
Harvard Law School

WITH REVIEWS AND CONTRIBUTIONS FROM

Dr. Adrian Gropper
HealthURL/ Patient Privacy Rights

Andrew Kim
Public Policy and Govt. Affairs, Google

Dr. Prashant Mathur
Director, National Centre for Disease Informatics and Research, ICMR

Dr. Roli Mathur
Head, ICMR Bioethics Unit

Leena Menghaney
Médecins Sans Frontières (Doctors without Borders)

Dr. Tony Raj
Dean, St. Johns Research Institute
Head, Division of Medical Informatics

Professor Suptendra Nath Sarbadhikari
International Institute of Health Management Research

Dr. Harpreet Singh
ICMR

Dr. R Sukanya
ICMR

Aruna Withane
APAC Strategic Trust Lead, Data Privacy and Compliance

Toshiki Yano
Head of Privacy and Security, Public Policy Strategy & Operations

KEY MESSAGES

- The data protection law should be all encompassing. A sector specific law on health data privacy may not be advisable given that the contours of health data are ever expanding.

- Health data may be best protected by a model predicated on accountability (to the individual); transparency; and portability. A model reliant on notice and consent is likely to fail.

- Emerging technologies like public blockchains will help all three goals – accountability, transparency and portability.

- Data controllers must have a fiduciary responsibility to the individual.

- Data must be considered personal and sensitive if their revelation results in discrimination, harm, violence or denial of services to the individual.

- Meaningful portability means portability of structured health data. The law must guarantee this, allowing time for implementation.

- Simple de-identification is likely to fail in this age of big data analytics and AI.

- Health data are best secured through anonymization and aggregation. Once aggregated, needless mandates for constant consent will be intrusive and will thwart clinical application, medical research and health tech innovation.

- Where explicit consent is required, it should be meaningful. The goal of notice should be to inform, not obfuscate.

- Patients may opt to (consent to) archive their data in one or more types of meta-directories that will then allow (or restrict) automated access for clinical, research, quality improvement, or marketing purposes. Separating the consent layer from data flow is key; it has been successfully implemented by India Stack while building the Universal Payment Interface.

- Cross border data flow is inevitable. Data localization is neither feasible nor advisable in this age of cloud computing. However, jurisdictional questions around accountability and redress need clarification.

- The law must embrace a flexible framework – technology is evolving at a rapid pace, and societal mores and norms are changing as well. What are considered sensitive data today may not be tomorrow. Individual comfort with processing of personal data may change with the advent of AI-based services, and the evolution of precision medicine. The law must allow for such changes, so as to not thwart innovation.

- Any exemptions made to the use of personal or sensitive data, whether under duress or in emergencies, should be subject to audit and review. This includes exemptions for national security.

- And finally, all progress notwithstanding, the law must protect individual rights – the right to privacy, the right to dignity, the right to be forgotten.

Our responses to 231 questions on the online portal have been submitted under "Satchit Balsari balsari@hsph.harvard.edu"

RESPONSES TO THE WHITE PAPER OF THE COMMITTEE OF EXPERTS ON DATA PROTECTION FRAMEWORK FOR INDIA

A LENS ON HEALTH DATA

HARVARD FXB
CENTER FOR HEALTH AND HUMAN RIGHTS

PART V
SUMMARY

Key Principles of a Data Protection Law

A data protection framework in India must be based on the following seven principles:

1. Technology agnosticism - The law must be technology agnostic. It must be flexible to take into account changing technologies and standards of compliance.

2. Holistic application - The law must apply to both private sector entities and government. Differential obligations may be carved out in the law for certain legitimate state aims.

3. Informed consent - Consent is an expression of human autonomy. For such expression to be genuine, it must be informed and meaningful. The law must ensure that consent meets the aforementioned criteria.

4. Data minimization - Data that is processed ought to be minimal and necessary for the purposes for which such data is sought and other compatible purposes beneficial for the data subject.

5. Controller accountability - The data controller shall be held accountable for any processing of data, whether by itself or entities with whom it may have shared the data for processing.

6. Structured enforcement - Enforcement of the data protection framework must be by a high-powered statutory authority with sufficient capacity. This must coexist with appropriately decentralized enforcement mechanisms.

7. Deterrent penalties - Penalties on wrongful processing must be adequate to ensure deterrence.

In order to achieve these principles, the Committee requests your views on the White Paper. The key issues analyzed in the White Paper and questions raised for consultation under each head are summarized below for convenience. We would be grateful if your answers are brief and targeted to the questions asked. Any other views on the subject will also be appreciated.

SCOPE AND EXEMPTIONS

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.

For a fuller discussion, see page 24 of the White Paper

Questions

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

   Our group's responses address the adequacy of the proposed framework for all "health data". Extra-territorial application of data protection laws must therefore apply. The understanding of what we consider "health data" continues to expand. Apps, wearables and telemedicine services now cross international borders routinely. Carrying on a business, or offering of services or goods in India are parameters worth incorporating in the law in light of international practices. Thus, an entity which does not have a presence in India but offers a good or service to Indian residents over the Internet, or carries on business in India may be covered under the law. It may also be worthwhile to consider applying the law to those entities that process personal data of Indian residents, irrespective of their location. This partially replicates the new EU GDPR formulation and puts the data subject squarely at the center of the legislation, ensuring that the law is made applicable to anyone who would processes personal data of the data subject. For health data in particular, while extra-territorial jurisdiction should apply to health services, the regulation on processing should address harm to the individual or to a group, and not be unnecessarily restrictive so as to thwart innovation or service delivery. There should, instead, be provisions that prohibit (and penalize) the use of health data to harm, discriminate, criminalize individuals or deny them services.

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?

   This is likely to be a regular feature of many health-related services: wearable devices and apps are a good current example. Services offered should be in accordance with domestic law, and should not result in harm to the individual. Market restriction is a plausible defense against harmful services. Entities must be held accountable without thwarting innovation.

   Concerns: The extent of jurisdiction may not be so wide as to constitute an unnecessary interference with the jurisdiction of other states or have the effect of making the law a general law of the Internet. For instance, the mere fact that a website (operated from abroad) is accessible from India should not be a reason for subjecting the website to Indian laws.

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

Alternatives:

a. Cover cases where processing wholly or partly happens in India irrespective of the status of the entity.
b. Regulate entities which offer goods or services in India even though they may not have a presence in India (modelled on the EU GDPR)
c. Regulate entities that carry on business in India (modelled on Australian law), business meaning consistent and regular activity with the aim of profit.

Option c may prove to be incomplete, because "non-profit" entities like hospital corporations in the United States have often observed to exhibit behavior consistent with corporations. The non- profit status is linked more to exemption from tax, than a direct correlation with intent or behavior of the entity. Also, the free service offered by WhatsApp (owned by Facebook) may not be considered a profit-mongering activity, except WhatsApp's and Facebook's business models are predicated on monetization of data. Similarly, in the health sector, various apps offer services for free but in exchange they collect a large amount of personal data. The app N1sighter, for example, even offers free consultations (in Rwanda and China, though based in the US). Such entities may argue that their activities do not fall under the ambit of data protection laws as the services offered are "free" and not with the aim of "profit".

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?

- A warning in writing in cases of first and non-intentional non-compliance and regular periodic data protection audits
- The EU GDPR provides for monetary penalty to ensure effective compliance of the law. The GDPR also imposes a fine of up to 4% of annual global turnover or €20 million, whichever is greater. A similar provision in the Indian context could provide for a strong deterrence mechanism.
- Failure to pay fines or to comply with any other sanctions imposed by the law could be linked to an order restricting market access.
- Mandatory establishment of a representative office (for ensuring criminal law enforcement) and holding the Indian subsidiary/related entity liable for civil penalties or damages may be explored.

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.

For a fuller discussion, see page 30 of the White Paper.

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?

(i) With respect to health data, data protection laws may be applicable to natural persons only. However, the law may be extended to juristic persons as well. The recent case of Strava App is worth noting in this context. The app allowed users to track and publish their exercise routes online. The company published a "heat map" of millions of users around

the world. The app was popular among US army personnel stationed in Afghanistan and Iraq. Given that usage of the apps among the locals was minimal to non-existent, the location of the US soldiers lit up, against a dark background, inadvertently revealing the location of the military base. Does the military have the right for its location (data) to not be published?[1] Similarly, trackers could identify where a health facility is located in a conflict zone by following cell phone traffic (data from cell phone towers called Call Detail Records). Publishing such data may harm the healthcare facility and make it vulnerable to attacks. Does the healthcare facility, a juristic entity, not have the right for its location data to not be published?

(ii) The law must apply to health data held by public and private entities. However, limited exemptions may be considered for well-defined purposes such as national interest, public health emergencies, disease surveillance, and research. Yet, we must be careful about how the concept of eminent domain is applied to data. There must be stringent criteria for application and the law must provide for a review process if exemptions are granted in emergencies or under duress. For health data, anonymized data may be exempted, provided processing does not result in re-identification. The volume of digital health data generated in India will be vast, and the potential for it to influence research and service delivery is real and tremendous. Thwarting the use of de-identified, aggregated, or anonymized data would be unfortunate. That being said, safeguards should ensure that entities (whether public or private) do not attempt to construct identified or identifiable personal data by combining data from multiple sources.

(iii) The law may have a transitory provision to address the issue of retrospective application.

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

   Alternatives:

   a. The law could regulate personal data of natural persons alone.
   b. The law could regulate data of natural persons and companies as in South Africa. However, this is rare as most data protection legislations protect data of natural persons alone.

   Option b. Companies have been known to withhold health-related information from the public. Corporations have long known about the negative health impact of their products before the public have been made aware. Can the law be applied to access such information from corporations, in this case the juristic entity, since the data relates to the health of individuals?

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.
   b. Have different laws defining obligations on the government and the private sector.

1 Richard Perez-Pena and Matthew Rosenberg, Strava Fitness App Can Reveal Military Sites, Analysts Say, N.Y. Times, (Jan. 29, 2018), https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html

Option a. Yes, the law should be common. Exemptions may be different for public and private sectors. Exemptions should be limited, and either established by community-consent and enshrined in the law; or require individual consent; and / or require formal review if exemptions made under duress or in an emergency.

Case illustration: In case of a highly contagious outbreak, a public health agency may want to utilize CDR data - call detail records (or cell phone tower data) from mobile operators, to see what cohort of individuals may have been exposed (in physical proximity) to an infected person. Traditionally this exercise, called contact tracing, has been done manually through interviews and observations, and is routinely practiced by the Centers for Disease Control (CDC) in the United States, and by public health agencies around the world. Now that CDR data can augment this activity, should public health agencies not be allowed to use the data, even if for a limited amount of time. We advise that one be allowed to do so, but only if several legal and technical tools are in place: consent, either pre-established or in real-time, community-wide or individual, as would be appropriate. Individual consent, in this case, could perhaps entail push notifications or text messages that offer opt-in or opt-out policies for tracking movement during an outbreak. That technical infrastructure should allow for transparency and auditing - it should be possible to review who had access to such data, for what amount of time, with what authorization and to what avail.

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.

Option b. Option a will be impossible to implement and prohibitively expensive in case of health data. However, the law must apply to future processing, even if data has already collected. Exemptions and special consideration may be required.

Case illustration: The law requires data portability. For healthcare, it may require that data for X number of years (retroactively) be privacy-compliant and portable. This may result in undue costs to small businesses and clinical practices. The law may need to make an exemption for such entities, or provide support, as was the case with the Affordable Care Act ("ACA") under the Obama administration in the US. The ACA mandated that health records be digitized, and provided remuneration to all providers that migrated their systems to standards prescribed by the ACA - a prohibitive proposition in the Indian scenario. For example, data portability as applied to health data, may require making patient data for X number of years retroactively portable. Regulations would have to consider the financial implications of such impact, and through additional policy making, provide for potential funds for such demands, if expected.

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?

Yes.

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

   There should be periodic review of the adequacy or limits of exemptions granted herein, to ensure that policy has kept up with evolving technology, and cultural acceptance.

3. Definition of 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.

For a fuller discussion, see page 34 of the White Paper.

Questions

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

   Use data to encompass both "data" and "information" as described above. Data should become personal if it inherently, or when combined with other data reveals the identity of the person in a situation where the person has not given permission or would not normally like their data to be linked to their identity. For example, GPS location on its own may not be personal data. But when GPS locations are tracked over a week, they may reveal the identity of the person. So, the definition should include the result of combined data that makes individuals identifiable. While it is important for businesses to know what kinds of data the law defines as "personal", it is important for the law to provide for hitherto unknown or evolving technologies, for example "facial recognition" as personal data. Illustration: In a restaurant in China, for example, the faces of guests are scanned (without their knowledge) while they are waiting to be seated, and their identities compared against a master list of global VIPs. The famous get to jump the line. The covert collection and application of such "personal data" to discriminate, punish or deny services is foreseeable and must be covered by the law. It is therefore imperative, that in addition to enumerating what kinds of data are personal, the law should also include the processing of data that results in re-identification.

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. Option b.

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?

   Data that reveals identity when identity ought not to be revealed (not the original intent of the individual or the data controller) should be considered as personal data. Age by itself, is not personal. Neither is gender. But age, gender, combined with profession and place of work may reveal identity, making the combination therein personal. Name, by itself, is personal. So are biometric IDs, which now include facial scans. The law must be

nimble and provide a mechanism for evolution in tandem with technological progress and cultural norms. If cell phone data are tracked to follow an individual, that is a clear violation of privacy. However, if anonymized cell phone signals are used to predict traffic patterns and identity is not revealed, the aggregated phone routes would not be considered personal data. On the other hand, GPS tracking processed to reveal an individual's visits to a mosque every Friday so as to determine most plausible religious belief, the GPS data, under those circumstances, should be considered personal. However, if CDR data is used to track traffic density and correlation with pollution, the same data is not personal. Further, "intent" should be factored in to determine if there was breach in protection from use of personal data.

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?

   Data should be classified as personal if it reveals the identity of individuals. Combined or processed data that reveal the identity of individuals should also be considered personal data. In the case of health data, for example, lab results or radiology images, in isolation, however sensitive and deeply "personal" to an individual, are not personal data in the legal sense, if they are completely de-identified, and more so if they cannot be combined or processed in any way to re-identify the individual. Therefore, in the case of health data, de- identified, anonymized data should not be considered personal (or even sensitive) until and unless identity can be revealed. Anonymized medical data have the potential to revolutionize medical science and healthcare delivery in India, and will need facilitating mechanisms to make such secure but seamless flow (exchange) of de-identified information possible.

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.]

   The law needn't recommend one or the other. Once anonymized, it should not be under the same restrictions as personal data, until such time that its processing or combining with other data, makes identification possible. Alternate view: 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. Therefore, pseudonymised data can't be outside the purview of personal data.

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?

   Yes. With the current technology, there are myriad different data points about us that "may" reveal our identity if processed or combined with other data points. It would be hard to enumerate them all, and harder to foresee what the future holds. The law

should therefore, in addition to enumerating what kinds of data it considers personal, prohibit the combining or processing of data that ends up generating identity from previously de-identified or anonymized data. It is important to consider intent in this context. If routine data processing results in inadvertent generation of identity, recourse should be available to the data processor to remedy its actions.

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

   Concerns: In the case of health data, the following issues may arise: Do data controllers of personal data have any obligations to act upon the personal data they have access to? "Personal" data in the health context may include genetic information, in addition to standard medical records. How and when may the state use personal or sensitive data that it has access to? Is the state obligated to tell the spouse of an HIV positive patient his or her status? Does the spouse not have the right to know, especially if the state (or private entity knows), and not knowing is a direct threat to his or her wellbeing? What about genetic disorders, in the case of adopted children? What if an entity has information about the existence of a highly inheritable cancer or a disease like Huntington's Chorea that may be devastating in the birth mother? Should this information be withheld from the adopted child? At what age should the information be made available? Whose consent? Should the recipient be made aware that information is available? Should they be allowed to seek it instead?

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.

For a fuller discussion, see page 41 of the White Paper.

Questions

1. What are your views on sensitive personal data?

   Sensitive personal data refers to data that individuals would like to be particularly private about. What constitutes sensitive data varies from culture to culture, and across time and space. Any data that subject individuals to any kind of harm should be considered sensitive. The more commonly accepted categories of sensitive data in the broad gambit of health or public health, usually encompass medical information, genetic information, sexual orientation, racial and ethnic origin, but could also include religious and political beliefs. Doctors Without Borders (MSF) consider a host of other categories of data as sensitive data: "i) Any data from which an implication of criminal conduct could be drawn and / or that can put MSF patients or research participants at serious risk (including death). This includes data on violence related medical activities, particularly, but not exclusively, in context of conflicts: 1) any data related to violence-such as bullet wounds and 2) any data related to sexual violence. ii) Data collected from MSF activities in prisons or any situation that are related to or can result in detention or deprivation of liberty (including insert and refugee a displaced person settings). iii) certain data variables such as those that could indirectly imply, truly or not, racial or ethnic origin, or political or religious opinions (for example, the origin or the location of the patient or participant) iv) Data related to sickness with an obligation to adhere to treatment 3) Data considered potentially sensitive by MSF (non-exhaustive): i) Data that can put the patients more participants at risk of stigma, discrimination, or criminal sanction

(including, in certain countries or populations, HIV and tuberculosis data). ii) Data on sickness or epidemic outbreaks".[2] One approach is to not get into the business of listing what data are sensitive, and instead describing what makes certain data "sensitive". Data that result in harm, discrimination, denial of service, jeopardy to life, liberty, or dignity, etc. However, such lack of clarity would make both the public and private sector uncomfortable, and subject to the vagaries of future litigants and litigation. It may therefore be prudent to adopt both approaches, to enumerate all categories of data that this law would consider sensitive, and provide for the inclusion of data not listed that should reasonably be considered sensitive based on its impact on individuals' privacy, liberty and dignity. The need for classifying data as personal stems from the need to restrict third-party access to such data. Data not directly considered medical data such as religious beliefs, caste affiliation or political beliefs could result in significant impact on healthcare, healthcare access, and other basic human rights. One should not assume that the public sector should have unrestricted access to such data. In fact, when not anonymized, there should be good justification for any identifying data from citizens that distinguish between or discriminate among various sub-populations. Once again, the law must provide for the list of data that its considers personal or sensitive to evolve as new technologies evolve, and with change in cultural and behavioral norms.

2. 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?

   [For instance, the EU GDPR incorporates racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.]

   Yes, the law should clearly define a set of information as sensitive data. Data concerning medical information, sexual orientation, political affiliations, religious or caste affiliations, etc. may be categorized as sensitive data. As discussed above, the law must provide for additional categories to be included, especially if data leads to harm, discrimination or denial of services. Every time sensitive data is accessed or exemptions are sought in order to access them, the entity, whether public or private, should be able to justify the need. Potential for abuse and harm is real. Case illustration: Knowing that certain neighborhoods have zero minority populations, may in fact shed light on possible discriminatory or exclusionary real estate practices. A responsible government may choose to intervene to protect minorities and promote their rights (and freedoms). Conversely, knowing where minorities reside may allow targeting them or excluding them from services. It may therefore be prudent to be more conservative with the use of sensitive data, and scale back restrictions as law and technology make transparency and information more accessible.

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

   Sensitive data may be subject to more restrictive notification and limitation norms. Data classified as sensitive may only be used for purposes originally intended for, unless explicit consent obtained. The document has only considered the Indian Medical Council Regulations, 2002 issued under the Indian Medical Council Act, 1956 and Clinical Establishments Rules. Other health related Acts, Regulations, Rules, Guidelines may also be considered: For example, Drugs and Cosmetics Act 1940 and Rules 1945,

2 Data sharing in a humanitarian organization: the experience of Médecins Sans Frontières, Issues in open research data 59, (2014)

and amendments from time to time, Mental Health Act, 1987, Consumer Protection Act, Prenatal and Preimplantation Diagnostics Techniques Act, Medical Termination of Pregnancy Act, Transplantation of Human Organs Act, Food Safety and Standards Regulation, 2011, The Pharmacy Act, Persons with Disabilities (Equal opportunities, Protection of Rights) 1995 etc, all have provisions related to privacy and data related to human health. The challenge will be to balance our concern with privacy and protection, with the vast (and positive) potential that big data, AI, mobile technology and cloud computing offer. Take for example, the ongoing study at the Onnela Lab at Harvard that conducts "smartphone-based digital phenotyping", the moment-by-moment quantification of the individual-level human phenotype in situ. Using data from personal smartphones, the lab focuses on modeling and forecasting psychiatric and neurological disorders. In other words, the phone's accelerometer is used to observe how different cohorts of patients move as their disease (Parkinson's or depression) progresses. Of course, consent undergirds all such studies and interventions. But who knew that the accelerometer data from our phones would end up being both personal and sensitive (may predict disease) and may, therefore, need to be protected. Again, the key is to keep the law nimble so that it may provide for such evolutions in technology.

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.

For a fuller discussion, see page 44 of the White Paper.

Questions

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

   Health data is almost always processed. For clinical use, health "data" are often combined with other data, or trended with previous versions of the same type of data, and shared with others based on clinical needs. For example, a new lab value may require that new specialists be consulted; or a certain reportable disease may require that public health authorities may be informed; or a certain kind of test result, may require the patient to be quarantined. For administrative use, health records may be routinely scanned for billing purposes. Usually, though these data are personal and sensitive, they are often not de-identified, when they could or should be. For example, billing departments in hospitals in India often have access to the entire medical record. This law should encompass and apply to all aspects of health data processing, requiring adequate privacy controls for personal and sensitive data, and allowing access to aggregated and anonymized data without undue burden.

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?

   Yes, the definition may list the three main operations of processing i.e. collection, use and disclosure of data. It may be worded such that it covers the operations/activities incidental to these operations, leaving room to incorporate new operations by way of interpretation. "Use" should imply analysis, application or the generation of an action based on the information. Manually collected health data are also sensitive (and personal), and must be subject to the same protections.

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.

   Yes, the scope of the law should include both automated and manual processing.

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

   Processing may also result in the "creation" of personal data. For example, by combining GPS location, other phone data, and wearable device data, software companies may be able to identify the individual to whom the personal fitness data belongs. Re-identifying data is not as hard as we think.[3] So, data that was not originally sensitive or personal may be combined to create highly specific personal data, that in turn could be sold to interested parties like insurance companies or business that want to sell health or fitness products or pharmaceutical products. Processing should therefore acknowledge not only the interpretation of data, but the creation of new data that may be personal or sensitive or both. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must also be as easy to withdraw consent, as it is to give it. The GDPR also provides for certain data subject rights like the right to breach notifications, right to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose, right to be forgotten, etc. which could be adopted in the Indian context. That being said, an architecture predicated on consent will not work, given the multiplicity of stakeholders in the health data ecosystem, and the large volume of interactions among various nodes in the system. What will work instead is an architecture predicated on accountability, transparency and portability. See future sections. Most health data in India are currently on paper and in simple digital spreadsheets. Maintaining confidentiality of these data is paramount in large population based studies. Government programs, ministries, research institutes like ICMR, Tata Memorial Cancer Hospital, and others have large datasets of personal and sensitive data. It is imperative that the law mandate provisions to handle these datasets with utmost caution. Anonymization and aggregation should be the norm, where possible. Until digitize and technical solutions installed, institutions may have to review their existing policies. The proposed NCD screening program by the Ministry of Health, for example, is to be rolled out across 19000 subcenters in India. Community workers will collect sensitive data on hypertension, diabetes and cancers from millions of households across India. Who has access to what parts of this information? Who decided this? What do individuals know and understand about this access? These kinds of questions need to be addressed while formulating the scope of proposed data protection laws. Additional notes: Consider the ICMR National Ethical Guidelines for Biomedical Health Involving Human participants, 2017. Section 2.3 on Privacy and Confidentiality states that Privacy is the right of an individual to control or influence the information that can be collected and stored and by whom and with whom, disclosed or shared. It also describes the

3 Larry Hardesty, We know where you live, MIT NEWS (May 17, 2016), http://news.mit.edu/2016/twitter-location-data-homes-workplaces-0517

obligation to protect or safeguard information from unauthorised use, access, disclosure, modifications loss or theft. In conducting research using stored samples or medical records or data, anonymization will be key.

6. 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.

For a fuller discussion, see page 48 of the White Paper.

Questions

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

   The data protection law should make a distinction between the roles of a data controller (organization which determines means and purpose of data collection) and data processor (organization processing data on behalf of the data controller). In case of health data, however, note that identifying the organization as one or there other may not suffice, as an organization may function as the controller of certain types of health data, and processor of others. This is an important consideration given that legal liabilities and obligations with respect to the protection of personal data would differ based on the role an organization is playing. The competence to determine the purpose and means of processing may be the test for determining who is a 'data controller'. The data controllers should primarily be responsible for complying with the law. The law may need to make an assessment of the likely impact of imposing obligations on processors and the compliance costs involved. Data processors should be responsible to take the necessary technical and organizational measures to secure the data they process on behalf of the controller. Industry experts reflect that the 'controller-processor' relationships are governed through contractual means and the law should not unreasonably intervene in these relationships. It is important to note that the Indian IT industry (acting as data processors) has been negatively impacted due to restrictions to the transfer of data under the EU Data Protection Regime. Section 43A of the Information Technology Act did not make a distinction between controller and processor with detrimental consequences to the industry. To address these concerns, the government later issued a clarification which helped create the desired distinction and exempted processors from certain requirements. The new law should avoid such a situation.

2. 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.

   The law must necessarily and separately define data controllers and data processors. Controllers should be primarily liable for compliance with the law, and processors for

their contractual obligations. All handlers of health data, however, whether controllers or processors should ultimately be accountable to the individual. Handling of personal or sensitive data by data processors may need additional protections (for the individual) under the law.

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

   Alternatives:

   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.

   Please see above

7. Exemptions

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.

For a fuller discussion, see page 52 of the White Paper.

Questions

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

   For health data, de-identified data may be used for bonafide purposes for clinical, research or administrative use, but in good faith, and not for actions that result in harm to the individual. Note, however, that big data analytics and AI make "re"-identification routinely possible, and prohibitions against such processing of data nearly impossible to enforce. Do not, therefore, use de-identification as the sole alternative for seeking consent. Aggregated data and differential privacy are better alternatives. There will be circumstances when entities may be allowed access to personal data, sensitive data, or both. For health data, disasters, public health emergencies, and individual clinical emergencies would be the most likely scenarios requiring exemptions, when data are not anonymized or aggregated. However, exemptions must be subject to purpose specification, use limitation, time limitation, audit, accountability and transparency. "National security" cannot and should not be used as a blanket defense to seek exemption, and should be subject to the same rules of accountability, transparency, audit and review. The law must provide for adequate security and organizational safeguards in the handling of such data.

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

Processing of health data under exemptions should have an articulated purpose (specification), time limitation, and be done in good faith for a bonafide reason (that may include clinical, research, public safety or administrative use). Broadly, any category of exemptions carved out under a data protection law will have to carefully balance the need for exempting a specific data processing activity with the plausible curtailment of the rights of an individual.

Domestic /Household Processing

1. What are your views on including domestic/household processing as an exemption?

   Individuals may opt to share digital health data within their ecology of family and relatives. For those that are not digitally literate, they may need to be provisions that allow (or disallow) the sharing of such data with certain family members. For health data, in particular, consider the following: It is common practice for several household members to be intimately familiar details of each other's medical problems, across generations. This cultural norm should however not result in defaults that risk the privacy, dignity and safety of the most vulnerable members of the household. Adolescent boys and girls, and women, for example should be able to seek medical care for sexual or behavioral health issues without their visits being shared with the household. Failing to do so would result in fear from seeking necessary care, or delay in treatment. This is a well-known, well documented phenomenon, and should be avoided at all costs. It may make sense for household access to health data to be a consent-driven opt-in policy, rather than the default.

2. Can terms such as 'domestic' or 'household purpose' be defined?

   The EU has formulated certain criteria to determine whether certain processing falls under personal or household purposes. These may be examined further for the purpose of articulating the exemption in law. However, the particular vulnerabilities raised by gender, sexual orientation and age, should be given careful consideration.

Journalistic/Artistic/ Literary Purpose

1. What are your views on including journalistic/artistic/literary purpose as an exemption?

   Journalistic use of health data should not trump an individual's right to privacy. As long as privacy is not breached, and individuals not harmed, journalistic use may be permitted (or even beneficial). Revelation or processing of health-related data for journalistic purposes should not result in worsening discrimination or violence against a group of individuals, or result in the curtailments of their freedoms, or denial of services to them.

2. Should exemptions for journalistic purpose be included? If so, what should be their scope?

   Yes. This may involve those activities where the necessity or purpose of the activity and the right to free speech and freedom of expression do not cause undue harm to or compromise the right to privacy of the data subject.

3. Would these activities also include publishing of information by non-media organisations?

   Yes

Research/Historical/Statistical Purpose

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

   The HIPAA laws (and their restrictive interpretation) in the United States have thwarted facile clinical applications and research. Data for research and statistical purposes seldom need to be identifiable, and consequently application of anonymized and aggregated data should be encouraged. All handlers of health data have a fiduciary responsibility to the individual. Technological safe guards would help ensure accountability, transparency and tracking of data as they travel from one processor to another. Use of identifiable data for "research or statistical purposes" may not be given blanket exemption, unless a bonafide reason can be provided, and the exemption is limited by time and use, and subject to audit and review. The law must provide for an effective intermediary to adjudicate such requests. We cover this in later sections.

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

   Yes, and in particular for personal and sensitive health data.

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

   No, good research will (and should) be published. Research may only be conducted under the ethical guidelines prescribed by the institutions controlling or processing data, as usually governed by ethical review boards at hospitals and universities. Industry and governments should be subject to the same ethical standards in conduct of health data processing. Monetization of health data requires additional regulation, given that health data are generated by a variety of entities including personal devices, medical equipment, pharmacies, labs, diagnostic centers, clinics and hospitals. The sale of personal or sensitive data should be explicitly prohibited, and additional laws are required to define the permissible sale of de-identified data. Such data also cross-national boundaries across corporations, and across servers. We will need specific policies governing the movement of health data back and forth across national boundaries in the inevitable cloud based ecosystem we will adopt. Blanket restrictions may be counterproductive. Recollect the announcement by Google, a few years ago, that they would provide services based on the content of our email in Gmail. While initially met with skepticism and resistance, a few years on, many users are quite happy to see their Calendars be auto-populated with their travel details drawn from itineraries mailed to their Gmail account. It is foreseeable that patients may well be happy with data drawn from their purchase of prescription medicine resulting in alarm reminder on their phone to take their medications on time. Or not. Comfort level with what is acceptable and what is not may evolved over time. Once again, the law should begin by protecting the vulnerable, but allowing for scaling back restrictions as technologies evolve, accountability easier to enforce, and cultural norms change.

Investigation and Detection of Crime, National Security

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

   This may not be a blanket exemption, as the potential for misuse (deliberate or inadvertent) by governments is real. There should be clear guidelines or parameters under which such exemptions may be evoked, by whom, for what time, and for what

types of data. Certain kinds of data may only be accessed with appropriate warrants or permissions. The law will need to specify who this granting authority (a "learned intermediary") would be. When an exemption is made during and emergency or duress, there should be mechanisms to audit the decision, or those affected to initiate inquiry or seek duress.

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?

   Yes, See above. The bandwidth for exemption may include 'prevention or detection of crime'; or 'apprehension or prosecution of offenders'; or 'assessment or collection of any tax of imposition of similar nature.' The exemption is available when the data is being processed for the above purposes, and complying with all data protection obligations such as giving privacy notices, subject access, rectification, data retention, etc. would impede the said investigation or apprehension/prosecution. Yes, any such exemption should be subject to strict safeguards, such as, a judicial mechanism to provide prior approval invoking such a clause, similar to the Court as envisaged under the Foreign Intelligence Surveillance Act, 1978 ("FISA") in the US. As far as health data is concerned, public health emergencies in particular, should be granted such exemptions, but also be subject to the same review and accountability.

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?

   For a health perspective, public health emergencies may be considered a national security issue. For example, use of de-identified lab data to track diseases may be considered a "routine exemption," or bonafide use.

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

   It may not be possible to conduct a manual review for each exemption. Privacy by design is key. Through intelligent design, automation and digital tracking of the use, transfer and application of such data, accountability can be maximized, and an audit possible. All exemptions should be audible, whether or not the audit is activated. The law would need to define how the learned intermediaries would be that would consider the audit, applicable to both the public and private sector, and the role of the judiciary, if any, in this auditing process.

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

   Through intelligent design, by employing emerging technologies, like block-chain that force transparency and accountability. Manual review will not work, given the vast quantities of health data constantly generated in India.

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

   Yes. Such matters may be referred to a designated authority or to the courts, unless the exemption is clearly articulated in the law.

7. Can the Data Protection Authority or/and a third-party challenge processing covered under this exemption?

   Yes. See 4 above.

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.

For a fuller discussion, see page 62 of the White Paper.

Questions

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

   We address two issues here: A) For health data, cross-border transfer of data is inevitable. Cloud based services and wearables provide a significant challenge. The regulation around wearable devices and apps is weak. For example, in the US, wearables are not considered "covered entities" under HIPAA, and subsequently HIPAA does not apply to them. Yet, wearables often have access to sensitive data include personal health data and geolocation. In an FTC study of 12 health-related mobile apps, the FTC found that these apps transmitted sensitive health conditions such as pregnancy, gender information, and ovulation information to 76 third parties such as ad networks and analytics firms. Consumer notice and choice should therefore be mandated of these devices and services, making market access contingent upon compliance. (What if individuals have purchased these devices overseas and brought them into the country?) Rules for such devices and services may incorporate Fair Information Practice Principles ("FIPPs") include: (1) collection limitation, (2) purpose specification, (3) use limitation, (4) accountability, (5) security, (6) notice, and (7) choice. Meaningful consent is discussed elsewhere. B) As far as "research" data and cross-border collaboration is concerned, data should be subject to the policies and ethics approval at the collaborating institutions. In today's era of cloud computing, federated storage, and multi-layered security, insisting on data localization (often interpreted and implemented as a local server) is short-sighted. The security model of leading cloud providers contains multiple layers of resiliency, redundancy and availability to prevent and mitigate the risk of security incidents and prevent such incidents from propagating throughout the network. Reading card computing solutions are often more secure than on premises are isolated data center alternatives. While insisting on date on localization, if at all, it is important to ensure that proposed local alternatives are at least on par technologically with professional cloud computing solutions. Eating cloud providers operate on a global scale using giraffe Khalid distributed infrastructure twin sure that services have maximum "uptime". Leading provider is conduct regular disaster preparedness exercise and execute numerous worst-case scenario is to ensure that services are redundant resilient and survive attacks.[4] It is important to address the ramifications of cross border data transfer when host country regulations are weak or governments turn hostile, and an examination of global treaties and norms in place to provide recourse, and protect the rights of affected individuals.

4 See e.g., Google Cloud Security and Compliance Whitepaper: How Google Protects your Data https://static.googleusercontent.com/media/gsuite.google.com/en//files/google-apps-security-and-compliance-whitepaper.pdf

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?

   The adequacy test envisaged under the GDPR could be adopted.

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

   Data localization is not necessarily a safer alternative.

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.

For a fuller discussion, see page 69 of the White Paper.

Questions

1. What are your views on data localisation?

   In general, data localization is not necessarily a better form of security. Data localization of all health data will be impossible, given the nature of mHealth services and devices, medical equipment data collection mechanisms, and even that of evolving electronic health records. It would be important to have laws in place that protect the individual's personal data irrespective of location of storage or processing. Please see response to Chapter 8 on why data localization may be short sighted, in the age of cloud computing and highly advanced layers of security offered by cloud computing services. Moreover, many health services will be cross-border by design, where data generated in India, through apps, devices and telemedicine, will be stored at one location, and analyzed at another (or several).

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

   It may not be feasible to do this for health data.

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

   A blanket call for localization for all sectors is detrimental. It would be technically difficult to implement in the context of health data. It is better to regulate access to the market by requiring compliance, data specification and accountability to individuals.

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

   See: https://static.googleusercontent.com/media/gsuite.google.com/en//files/google-apps-security-and-compliance-whitepaper.pdf for an explanation of why professional cloud computing services are better alternative (right now) than local servers with perimeter security.

10. Allied Laws

Currently, there are a variety of laws in India which contain provisions dealing with the processing of data, which includes personal data as well as sensitive personal data. These laws operate in various sectors, such as, the financial sector, health sector and the information technology sector. Consequently, such laws may need to be examined against a new data protection legal and regulatory framework as and when such framework comes into existence in India.

For a fuller discussion, see page 76 of the White Paper.

Questions

Comments are invited from stakeholders on how each of these laws may need to be reconciled with the obligations for data processing introduced under a new data protection law.

Other laws having provisions related to privacy and data related to human health: · Drugs and Cosmetics Act, 1940 · Drugs and Cosmetics Rules 1945 · Mental Health Act, 1987, · Consumer Protection Act, 1986 · Prenatal and Preimplantation Diagnostics Techniques Act, 1996 · Medical Termination of Pregnancy Act, 1971 · Transplantation of Human Organs Act, 1994 · Food Safety and Standards Regulation, 2011 · The Pharmacy Act, 1948 · The Persons with Disabilities (Equal Opportunities, Protection of Rights and Full Participation) Act, 1995

GROUNDS OF PROCESSING, OBLIGATION ON ENTITIES AND INDIVIDUAL RIGHTS

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.

For a fuller discussion, see page 78 of the White Paper.

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.

   For health data, consent needs to be layered. Consider the following use-cases: A patient admitted to Hospital X has records in Hospital Y. The patient is gravely injured and unable to provide consent. Hospital Y should be allowed to provide access to Hospital X without written consent. Consent should be "implicit" in the best interest of the patient. An oncology practice has 10 years of data on clinical outcomes for various treatment protocols for certain types of cancer. Should they be allowed to participate in a multi-center analysis looking at these data, if all the data are de-identified? Why would consent be necessary? Should the institutional review board not suffice? What if data entered into a fitness app is being sold to a third party in a different country, so that services can be targeted to the individual? Clearly consent should be required? What is a hospital wants to know how well they are doing with managing patients with diabetes, heart disease or HIV, by following their HgA1c, blood pressure or CD4 counts, for example? As an internal quality control exercise for their doctors? How much data should they be allowed to review and not? The whole record? De-identified data? Specific parameters? Is consent required if data are adequately de-identified? In general, clinical care and research will be negatively affected if consent to access health data is onerous, although health data are probably the most personal and sensitive of all data. Standards for consent will need to apply across private and public healthcare delivery organizations, but will need to be forward looking, as more and more medical care delivery is either automated, tracked remotely, or provided via telemedicine.

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?

   Consent for health data may be implicit (or not required) when it fulfils other criteria including legal or contractual obligation. In certain cases, exemptions for consent will also need to be determined by local laws: should spouses of HIV positive patients be informed of the HIV status, without the consent of the patient? By for the most part, consent for health data, when explicitly sought, will need to be unambiguous when the data is identifiable. EU GDPR guidelines should be applied in the Indian context,

requiring consent to be meaningful and accessible. For example, people may need audio or visual aids to compensate for illiteracy, or should have a right to be informed about the consent process in their first language.

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

   In medical practice, it is often required that care instructions given to patients be written in plain language at school level literacy. It is conceivable to think that laws may require a simple articulation of data use practices (limiting word limit), and providing feasible alternatives when screens do not exist, for example, in the case of wearable devices like fitness trackers. Audio and visual aids, multimedia clips, are all feasible options. Technology should allow users to choose from a menu of options for health-related data and allows them to withdraw or provide additional consent at will. Simple messaging and menus, as available with most apps on both the Apple and Android platforms, would allow users to consent and control access: should their health data be used for a) their clinical care b) hospital quality improvement initiatives c) research d) marketing for services to them e) marketing for other purposes, etc. As with the Universal Payment Interface in India, separating consent from data-flow in time and space will make the acquisition (and application) of consent feasible at scale. Block-chains will enable the application of consent preferences, but importantly will make data flow transparent and traceable across all nodes of the health data ecosystem. Technology would also make it feasible to gain community consent (or individual consent) for secondary use of data not originally envisioned. Such secondary use may be allowed via notice, or opt-in, opt-out options. Again, enforcing accountability may be more feasible than requiring consent. Onerous consent requirements when data are anonymized and individuals are not harmed, may significantly thwart innovations. To address fatigue and multiplicity, minimize the number of times consent is required by replacing the consent architecture whenever feasible by that of aggregated data and transparency. The underlying principle should once again be that of accountability to the individual. As far as the use of health data for research is concerned, it is still very much under the purview of various ethics boards and regulations at research institutions (hospitals and universities). So far, ethics boards have managed to extend their scope of oversight to research with new forms of data (including, for example, data from cell phones) and devices. Research conducted by businesses on data they acquire (or purchase) should only be under the purview of the law if the data is identifiable, or if the processing will result in identifiable data that would subject the individual to harm. Again, the law must ensure that there are provisions that allow the consent architecture (and principles) to evolve with technology and cultural shifts.

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

   See above. It would be important to determine who constitutes the “data controller” in case of health data, that are generated by a variety of players, ranging from hospitals to phone apps.

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

   Yes. In the case of digital health data, data would be best protected by design. Allow automated but consented flow of data. Consent can be layered. Prohibit unconsented data flow, or monetization of personal or sensitive data without consent. Any future use of health data, especially if de-identified, should be governed by local ethical

regulations and standards. Use of de-identified health data should not be needlessly restricted. The potential for medical advancement given the volume of data the Indian healthcare system will generate, is vast.

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

   If there is any risk, whatsoever, to the individuals' safety, dignity or privacy, or if data processing will result in discrimination, violence, harm or denial of services, meaningful consent must be explicitly sought, irrespective of the burden.

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.

For a fuller discussion, see page 85 of the White Paper

Questions

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

   Processing of children's health data, for purposes outside of a legal or contractual obligation, may need higher level of scrutiny and consent. Restrictions should not preclude children and adolescents from accessing health information or health services in privacy, especially services that affect that sexual or behavioral health.

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

   For health data, yes. Especially if devices and apps provide services to minors. That being said, we don't want to prevent minors from accessing services that would be useful for them, for example, adolescent counselling or sex education or support groups, and such. Again, processing of data acquired through such services may be easier to regulate, than trying to regulate consent.

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?

   With regard to health data, all children below 18 years of age should provide assent and also parental consent. Those above 18 years can provide only consent as adults. The concept of Informed assent exists in research studies where confidential information is collected from children, in addition to informed consent from the parents/legal Guardian. Ref: Informed consent/assent in children.[5]

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?

   Access to data from minors, for now, may require more explicit consent than would be acceptable among adults. This may however be hard to enforce given how healthcare

5 Statement of the Ethics Working Group of the Confederation of European Specialists in Pediatrics (2003), https://www.ncbi.nlm.nih.gov/pubmed/12884032

services will be delivered in the future, through personal mobile devices, apps, the internet and so on. It may be better to hold service providers accountable, instead of solely relying on a consent or assent architecture.

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?

   A case-by-case approach would be too onerous given the projected exponential growth of online medical services. Not sure if this approach will work in India and may perhaps be open to misuse by data controllers.

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
      The entity collecting the data may conduct the test, but will be subject to audit and review by the data protection authority to ensure that such data collection resulted in no harm to the child (or his/ her family or community).

7. 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?

   No, they should not be exempt, especially if they are aware that the users are minors. Services providers should be expected to put additional safeguards in place to ensure that users are not minors of their data processing results in a) the use of personal data, and b) any potential harm to the minor, now or in the future.

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.

For a fuller discussion, see page 92 of the White Paper.

Questions

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

   For health data, notice is important, but cannot be the only mechanism for operationalizing consent. Sometimes, notice won't be possible. Often times, notice

may be inadequate. When notice is required, it must be accessible to those with poor literacy, and include audio visual aids. Laws should favor the individuals and require opt-ins instead of opt-outs, when there is any concern about the individual's capacity to understand the notice. However, as far as possible the architecture of the health data ecosystem should not rely on notice and choice. Instead, consider separating the consent layer from data flow, as in the case with UPI. An API-enabled ecosystem that employs public blockchains will ensure transparency, accountability and portability - the mechanism of choice for operationalizing consent.

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?

   When notices are required, they should be simple, and standardized. Researchers are used to standard nomenclature with services like Creative Commons that offer a variety of licensing options for one's creative work that ranges from open access to highly restricted reproduction privileges. Similarly, developing standard categories of consent in health data may be advisable, where - over time - patients know that they have the option to store their data in one of the three of four different kinds of meta directories: databases that allow use of their data only for their clinical care; databases that allow quality control operations; those that allow research; those that allow marketing; and so on. The default should be one that protects the rights of the most vulnerable, and those with limited digital or health literacy.

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

   Yes

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

   Alternatives:

   a. No form based requirement pertaining to a privacy notice should be prescribed by law.
   b. Form based requirements may be prescribed by sectoral regulators or by the data protection authority in consultation with sectoral regulators.

   Yes. B. Again, as far as possible avoid the need to provide notice. Instead, ensure privacy by design. Make it technologically necessary to guarantee transparency, accountability and portability (see sections on enforcement).

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?

View 1): Data trust score assignment may not be feasible given the sheer volume of players in the health sector.

View 2): Consider certification of the services on the lines of the Honcode certification used for trusted medical information on the internet. The proposed certification may rank the quality of meaningful notice, influencing users' decision to trust the services.[6]

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?

For health data, this may be conceivable. Block-chain may allow users to see where their data resides, or has traveled. They may be a able to investigate what kinds of data a particular processor has access to. Realistically, this may only be applicable to personal data. Given the extensive processing and reprocessing of health data, it may not be feasible (and not necessary) to track migration of aggregated data. We introduce here the concept of a notice bank. To avoid consent fatigue, what if users of health data had a notice-bank that they voluntarily logged into? The notice-bank would not be allowed to hold opt-out notices; only opt-in notices. This prevents constant privacy invasion. It is up to the user to visit the notice-bank. They may be incentivized to do so by the services that have posted the notices. This may be useful for secondary uses of data for direct marketing or selling of data. At all times, it is preferable instead to avoid the need for constant consenting, and have users choose upfront one or two kinds of meta directories that they would like their health data to be stored in (see above). Let us go back to our example of epidemiological surveillance: there is a disease outbreak that is expected. The government wants all labs to share data about positive lab tests for disease X. Not the patient's name, but only the positive or negative result, and zip code. It may be reasonable to think that this is a legitimate use of data for public safety, without jeopardizing the individual. Now imagine the disease is contagious like Ebola. Should everyone in the vicinity of the zip code receive a push notification on their phone saying they may been exposed? What if it is well known to the neighbors that person M may have travelled to an endemic area and conclude that s/he is likely the culprit, and begin to ostracize them publicly? These tensions between health, public health, rights and dignity must be resolved either through legal or technical solutions engineered into the use of such data. Notice can become burdensome. Some notices need a timely response, some not. Could we imagine a system where secondary data like the one above (outbreak surveillance) either does not need consent, or sends out an opt-out notice, "We are in the middle of an outbreak, and the public health agency would like to use your lab data to conduct disease surveillance. Your identity will not be shared. If you do NOT want us to share this data, you can opt-out by texting "NO" to this number within 24 hours of receiving this notice." However, notices by companies trying to apply your data to other purposes, or sharing or selling them, may be too many and too disruptive. What if they are required to send notice to a "notice bank" that individuals are free to peruse. Notices in notice-banks should be opt-in notices. If companies want the data desperately, they can incentivize customers to scroll through their notice-bank. The notice bank may have all sorts of notices awaiting consent, from old and new data: "The results of your CT scan from 2005 are being requested by an AI company trying to automate radiology reads in the future. Your identity will not be revealed, but other lab results and diagnoses may be requested. Do we have your permission to share this data with the device company? We are offering Rs. 1500 to you in compensation for this secondary use of your data" Should money be allowed to buy personal data? "We are offering Rs 3000 to you in compensation if you also give

6 See Honcode, http://www.hon.ch/HONcode/Patients/

us permission to share your contact information with the company" Is this coercive? Exploitative? Especially among vulnerable populations? We do not believe that layered consent with hyeprlinks is either practical or ethical for the Indian population given its level of digital literacy. Layered consent is a cop-out, even in the West. Consent fatigue is real, and consent is meaningless if not designed to inform and protect the individual, rather than fatigue her to acquiesce.

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

   Easy to read; consider audio visual aids. The purpose of notice should be to inform, not obfuscate. These notices are particularly important in case of devices and apps where there is no "norm" or expectation of what the companies will do with the data (as would be the case with hospitals, or individual practitioners). Personal health data from wearables, "IoT" devices, smartphone apps and other similar modalities should be under the purview of the law. Purpose (and type) of data collection should be clear to the lay user ("pictures uploaded during your telemedicine consult will become our property, and used to better our AI algorithms," etc.). Any subsequent change in intention should require consent, unless the data are aggregated and anonymized.

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.

For a fuller discussion, see page 99 of the White Paper.

Questions

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

   In case of health data, consent should underpin all transactions. Consent need not, however, be explicit or in real-time. Nor should processing be restricted if health data are anonymized or aggregated. If processing results in making data re-identifiable, even if inadvertent, notice must be given, and consent sought, failing which the controller and processor should be required to destroy personal data they are not authorized to use. Grounds for processing health data will vary. An emergency department should be allowed unfettered access to an unconscious patient's health data. Now assume the patient is HIV positive and does not want the doctor to know. Not knowing the patient's HIV status puts the care team at risk, and under these circumstances, it should be permissible for the hospital to access the patient's data in toto – but only for the purpose of emergency care (use limitation, as discussed in the next section). Processing personal data or sensitive health may be allowed without consent when permissible by law. These exemptions should be granted selectively, and such processing should be subject to audit and review, if not enshrined in policy.

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

   We provide here examples to consider in the health context for the criteria followed by the EU: (i) Performance of Contract: User downloads an app that will alert her

to the need for updating vaccinations based on her travel itinerary and her current vaccination record. The app would require to access the user's medical record. It may, in the future, may even draw from the user's email to predict future travel based on any stored itineraries in the email. If the user has agreed to these features, the app is performing its contractual obligations, and no explicit consent should be required every time. However, the app should not be allowed to process the data for other purposes, or be allowed to sell the user's medical information to a third party, without consent and notice. Question: should the app be required to treat information about the patient's health records and patient's travel itinerary as distinct types of data? We believe yes. The company may choose to sell the user's travel data to vendors who may want to market travel services (hotels, cars) to the user based on their data, provided the user knows that their data may be shared or sold. (ii) Legal Obligation: Law may mandate physicians to report certain diagnoses to the state, for example or may require laboratories to share de-identified results of certain diseases when there is fear of epidemic outbreak for surveillance monitoring. It is important to ask who makes these laws, and how patients may have a voice in the formulation of these policies. It is easy for the state to gain access to personal health data, citing legal obligation, unless parameters for such access are well defined. (iii) Vital Interest: In case of health data, this needs to be well teased out. While access to a patient's health data to protect his or her own health is understandable (as in case of emergencies), it is harder to determine when health data may be accessed to protect the life of another individual. For example, the spouse of an HIV positive patient; or the offspring of a patient with an inheritable disorder. (iv) Public Interest Task, Exercise of Official Authority: An even more slippery slope. This provision will allow the state to by-pass usual checks and balances and should be used judiciously, especially while handling health data. There need to be clear guidelines (by whom) for either allowing such bypass, or a formal post hoc review process. Public health emergencies should be considered a vital interest. But at any point, if access to health data risks limiting individual freedoms or rights, global norms (such as the Syracusa principles in regard to quarantine, for example), and domestic law should be carefully examined. While it may be okay to use, say, CDR data to trace contacts during a high mortality epidemic, it may not be okay to use information about HIV status or sexual orientation to quarantine, target or discriminate individuals. It is not inconceivable that some of these actions may be considered as protecting public interest by certain groups of people, though a blatant violation of human rights, and domestic law. (v) Legitimate Interest: For health data, legitimate interests may cover use of data for research purposes (but should be under the purview of institutional ethics board), or quality control and administrative purposes, etc. Such applications of data should not risk the health, dignity or life of the individual. The patient's best interest trumps.

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. A case-by-case exemption is impractical. Criteria should be agreed upon based on global and domestic norms, in the best interest of the patient, and / or based on new health data protection laws. The data protection

authority (?) may lay down 'lawful purposes' by means of a notification.

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

   The application of block-chain technology to control, access and tag health data seems like a plausible option in the near future. Domestic laws will need to protect populations that cannot interpret what they are signing up for. Laws should be in favor of the patent's privacy, and should trump the needs of the private sector, and perhaps, even the public system, when possible. And yet, when data is not identifiable, allowing big data processing and application of AI, will help accelerate research and health care innovation. The processing of certain kinds of personal data without consent may become permissible in the future, as we discussed above with the example of Google Calendar and Gmail; or the patient's whose data from her medicine purchase activated her phone reminders. It is also important, in the case of health data, to consider the particular case of the patient unable to give consent - too debilitated, or is unconscious. Adequate provisions need to be made, in the coming digital era, to access personal data of and for such patients. Failure to do so may result in actions not taken in accordance with the wishes of the patient. The concept of the healthcare proxy is underdeveloped in India, and needs legal and societal attention.

5. Purpose Specification and Use Limitation

Purpose specification and use limitation are two cardinal principles in the OECD framework. The principles have two components- first, personal data must be collected for a specified purpose; second, once data is collected, it must not be processed further for a purpose that is not specified at the time of collection or in a manner incompatible with the purpose of collection. However, the relevance of these principles in the world of modern technology has come under scrutiny, especially as future uses of personal data after collection cannot always be clearly ascertained. Its relevance for the Indian context will thus have to be assessed.

For a fuller discussion, see page 105 of the White Paper.

Questions

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

   Purpose specification and use limitation are very relevant to health data. Narrow definitions of either, in the context of health data will stymie clinical care and research. Unregulated use will lead to abuse, as can be imagined with the vast amounts of personal and health data collected by apps and wearables. It may therefore be important to differentiate between types of health data and the various data controllers involved in the health data ecosystem. Should traditional data collectors like hospitals and labs, for example, be given more freedom to make secondary use of data, provided the use would be considered reasonable? Should private entities and product companies that own apps and wearables be treated under different standards? Who will regulate them, and how? Especially, when the data collected are likely to cross borders? Should their use be limited to the purpose specified, and exemptions be allowed on a case by case basis? Who will bear the burden of making these exemptions? Alternatively, as long as data are not personal, and cannot be identifiable, why not allow innovative processing and application of data to fully harness the benefits of big data analytics? We submit that purpose specification and use limitation principles are particularly

important while handling personal data, and less so when dealing with aggregated data. However, with progress in the science of precision medicine[7], accessing personal data may prove quite beneficial to the patient. Where purpose specification and use limitation cannot (or should not) be applied, consent, accountability and transparency should be employed.

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

   Purpose specification and use limitation principles if applied rigorously would slow research and innovation in healthcare. In circumstances when these restrictions are relaxed, consent may need to provide counterbalance. For example, if the smart phone develops a feature, that prompts you to exercise more based on your mobility pattern, you may like it. However, if it sells these data to an insurance carrier who in turn raises your premium, the app would have acted unreasonably and not in your best interest. What if it wanted to use these data to suggest discounts available at the nearest fitness centers? You will probably want the app to get your consent before it starts using your mobility data to send you marketing notifications. This is one example - now consider the Internet of Things. The possibilities presented by an army of such devices on and around monitoring how you breathe, eat, drink and move, are endless, exciting, and matched only by their potential for abuse and invasive control.

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?

   Gap between data protection authority and end user should be filled by establishing a central authority (e.g. Banking Ombudsman). Every data collector and processor should maintain a repository of purpose specifications that they are authorized to collect from a legal authority. This authority should be empowered to inspect, verify and receive complaints if data is reasonably compatible or if any deviations in purpose have occurred. Such authority should also help set standards. An alternative view we submit is that subsequent use of health data not necessarily be compatible with initial purpose. Data about water quality, soil safety, air pollution and myriad other parameters in our environment may be relevant to our health, and may be combined with our personal data to build predictive models about our health, or propose alternate routes or food or travel choices. Conversely, aggregate lab data on malarial smears may be used by a public health agency to monitor outbreaks. It is better to ensure that subsequent processing does not harm the individual, rather than restrict processing, especially of anonymized aggregated data, even though it may be processed for a purpose different from the original intent. These standards will require to evolve, and restrictions may also be scaled back as security, encryption and user demand dictates.

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

   Alternatives:

   a. The sectoral regulators may not be given any role and standards may be determined by the data protection authority.
   b. Additional/ higher standards may be prescribed by sectoral regulators over and above baseline standards prescribed by such authority.

7 U.S. National Library of Medicine, What is Precision Medicine? https://ghr.nlm.nih.gov/primer/precisionmedicine/definition

c. No baseline standards will be prescribed by the authority; the determination of standards is to be left to sectoral regulators. Health data are more personal and sensitive than most other kinds of data, but also need the most processing. Their secondary (and tertiary) use holds great potential for advancing clinical care, research and delivery.

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

The purpose of collection of personal data must be provided at the time of collection of data. We raise two concepts here, that are often the norm in public health research: Return of Results and Benefit Sharing - It is important to communicate back to providers of data (individual or communities) new findings that may be of relevance to them. Benefit sharing: Data may have potential commercial value and efforts to be made to provide access to products, tests, discoveries and share benefits with original donors. Appropriate community engagement with relevant stakeholders may also be required to build public trust.

6. Processing of sensitive personal data

If 'sensitive personal data' is to be treated as a separate category, there is a concomitant need to identify grounds for its processing. These grounds will have to be narrower than grounds for general processing of personal data and reflect the higher expectations of privacy that individuals may have regarding intimate facets of their person.

For a fuller discussion, see page 111 of the White Paper.

Questions

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

Like in the case of EU, UK and South Africa, this should be prohibited and only under stringent regulations be allowed to process with due consent and authorization of each data owner. Data protection authority should be careful about processing of personal data having information on political opinions, racial or ethnic origin, religious or philosophical beliefs. Alternate view: Health data are reflexively categorized as sensitive. But is this really the case in the era of digital health data where de-identification, anonymization and encryption are routinely possible (though not yet practiced in India). Until technical safeguards are in place, the law should protect individual's sensitive data through use limitation. But it is imperative that the law allow provisions that will scale back such restrictions once technological solutions allow for processing large amounts of anonymized data, and eventually in the case of precision medicine, perhaps even personal data. While carving out a separate regulatory authority for health data is tempting, it is hard to identify the contours of what constitutes health data. A current study at Harvard, for example, monitors the accelerometer in one's phone to monitor motion and activity to predict patterns of illness. Phone accelerometer data would not typically be considered health data – however, in this case, it is.

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?

In addition to the specific categories in the UK, US and South Africa, Aadhar number, caste, sexual preference, and Voter ID details must be included in the Indian context. Any data that risks discrimination of an affront to the individual's privacy, safety or dignity should be considered sensitive.

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

   Alternatives:

   a. Processing should be prohibited subject to narrow exceptions.
   b. Processing should be permitted on grounds which are narrower than grounds for processing all personal data.
   c. No general safeguards need to be prescribed. Such safeguards may be incorporated depending on context of collection, use and disclosure and possible harms that might ensue.
   d. No specific safeguards need to be prescribed but more stringent punishments can be provided for in case of harm caused by processing of sensitive personal information.

   Prevention by design. Make it technologically unfeasible to exploit sensitive data without requisite permissions or policies in place. Until such technology can be universally scaled, categories of health data that are likely to result in harm or discrimination if shared without explicit consent of the individual should be accorded more protection, through stringent use limitation and consent requirements. When in doubt, err toward more protection than less. Time and technology will permit the scaling back of such restrictions. Ensure that the law allows provides for revisiting these norms and categories in pace with evolving technology.

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?

   It is hard to identify the contours of what will constitute "health data" in the future. It is better to describe limitations on the basis of the impact (harm) that processing of various kinds of data would cause.

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

   Currently, medical research often requires the handling of sensitive personal data. Within our public health system, large public health interventions like the NCD screening program mentioned above also handle unprecedented volumes of sensitive and personal data. Manual review, consent and notice, etc., are impossible to enforce. The law must require that sound technological safeguards are instituted while handling such data. Once again, privacy by design will be a lot more effective than a consent and notice system. With the advent of Precision Medicine, the healthcare system will be forced to handle an even larger amount of personal data that it is already used to—the law must be forward looking and accommodate for the inevitable processing of personal sensitive data, at scale.

7. Storage Limitation and Data Quality

Related to the principle of purpose specification is the principle of storage limitation which requires personal data to be erased or anonymised once the purpose for which such data was collected is complete. Personal data in the possession of data controllers should also be accurate, complete and kept up-to-date. These principles cast certain obligations on data controllers. The extent of such obligations must be carefully determined.

For a fuller discussion, see page 117 of the White Paper.

Questions

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

   Health data, intuitively, require to be stored for a longer period of time than many other data. At least, for the lifespan of the individual, if not longer. Healthcare systems in developed digital economies have had to invest hundreds of millions of dollars in warehousing digital health data (and securing and duplicating them). Health care institutions (public and private) will need to negotiate how data is stored and who pays for this storage. A federated storage system where data is stored at source but can be easily called up, is likely to be the most feasible.[8] For health data, it may become necessary to specify time period for storage with all identifiers. If newer processing methods are envisaged, then data has to be anonymized and archived. There are models for doing this safely.[9] Re-identifying of data, when possible, would need to mandate exemption, or consent. Conversely, there need to be standards about data destruction as well, that may, at times entail physical shredding of storage media. As far as quality of data goes, there are well established, locally adopted universal norms for standardization and interoperability.

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

   Given the sophistication of health data, the burden of accuracy of health data falls on the data collector and processor, within reasonable limits. Data collectors cannot however be responsible for false information supplied or information withheld by patients.

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

   Alternatives:

   a. Data should be completely erased
   b. Data may be retained in anonymised form

8 https://cyber.harvard.edu/events/digitalhealth/2017/01/Gropper (Current popular models being proposed in India call for a central warehouse of all patient medical records. These are likely to be prohibitively expensive and most vulnerable to security breaches)

9 SAIL Databank used by Swansea University, https://saildatabank.com/about-us/overview/

For health data, this would depend on the kind of data, and the costs associated with storing the data. Lab data, radiology data, tissue samples all need to be stored for varying amounts of time. Consent and transparency around this process would allow individuals to know how long their data will be available, to whom and in what form. Anonymized or aggregate data may be stored for longer periods of time or processed forward.

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?

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

   View 1) Personal health data are sometimes parsed by cloud service providers, by scraping relevant information. Such unauthorized use of personal data should be prohibited and would require application of domestic law to cross border services.

   View 2) Apart from data completeness and accuracy of data we must also focus on consistency of data. Consistency refers to the absence of apparent contradictions in a database; redundancies may therefore be allowed to some extent.

8. Individual Participation Rights – 1

One of the core principles of data privacy law is the "individual participation principle" which stipulates that the processing of personal data must be transparent to, and capable of being influenced by, the data subject. Intrinsic to this principle are the rights of confirmation, access, and rectification. Incorporation of such rights has to be balanced against technical, financial and operational challenges in implementation.

For a fuller discussion, see page 122 of the White Paper.

Questions

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

   It is important to be transparent and permit individuals to access their personal data. Technology would be the key determinant in India's ability to apply such individual participation right. Public block-chains, use limitation and consent-and-notice norms would allow individual participation. An individual should be able to review all her data tagged as health-data or health-related data, and should have the ability to petition the data processor for change. The fee for processing may be refundable if the error was found to be the data collector or processor's. More granularly this is probably best handled at the decentralized level. Individuals should have access to their health data when they are generated (lab reports, physician notes, etc.) and have the ability to rectify or challenge them. The challenge is with processed health data. How do individuals access secondary or tertiary data about them that companies may have generated by combining data from various sources? An individual should also be able to conceal certain sensitive personal data from her provider if it is not relevant to her care. An expert entity will need to agree on what kinds of data can be concealed or erased without jeopardizing individual, provider, or public safety.

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

No, all shared personal data should be accessible. However, in the case of health data, it may be difficulty to operationalize the individual's right to access data processed for secondary purpose. Individual participation may not be applicable to anonymized or aggregated health data.

3. What should be the scope of the right to rectification? Should it only extend to having inaccurate date 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?

These provisions should be worked out at the source at which data is generated. If rectified, the onus of communicating changes to all entities that the data collector may have passed on the data to, should lie with the controller and not the individual. Individuals should be allowed to withdraw consent and remove most data (with a few exceptions necessary for personal safety - like allergy list, unless there is an error; or for public safety like the presence of a contagious disease, like TB).

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/sectoral regulators may prescribe a reasonable fee.

A fee structure may be layered. For most request, there should be no fee. Repeated changes may entail some charges. Fees may be charged if data errors were not due to lack of meeting contractual obligation nor from error on part of the data collector or processor.

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

Yes, there should certainly be a time period for response, prescribed by law, policy or contract. The time period will depend upon the type of data and purpose of request

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?

While technically feasible, it may not be legally feasible. We are essentially asking here for companies whose future is predicated on intellectual property rights over cutting edge AI algorithms. When such automated decisions affect clinical care, they will have to come under the same rigorous standards as clinical trials, and will have to generate evidence (and agree to transparency) to back their claims. When such automated decisions result in discrimination or denial of services, individuals should have a legal right to access the logic, and to seek recourse. But it is likely that the next generation of automated decisions are likely to be recommendations for health and lifestyle

modifications, and other benign services for which the right to access logic may not be necessary. The right to know what data are being used is a different matter, and may be exercised. Customers have a right to know if and how personal data are being used. Time and energy may be better spent on defining what kinds of applications of such automated decisions are permissible.

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 organization is a private body or a public body.]

   The UK approach is reasonable.

9. Individual Participation Rights – 2

In addition to confirmation, access and rectification, the EU GDPR has recognized other individual participation rights, viz. the right to object to processing (including for Direct marketing), the right not to be subject to a decision solely based on automated processing, the right to restrict processing, and the right to data portability. These rights are inchoate and some such as those related to Direct Marketing overlap with sectoral regulations. The suitability of incorporation of such rights must be assessed in light of their implementability in the Indian context.

For a fuller discussion, see page 129 of the White Paper.

Questions

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

   The right to object to processing of personal data, and the right to object to processing for direct marketing are reasonable demands. Some health data, even though personal, may not be concealed or deleted, as discussed in the previous section. The right to restrict processing may be more feasible in the context of health data, as would be the right for no healthcare decision being made solely on automated processing. Health data portability is key and must be interpreted as portability of structured data.

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?

   For health data: Data portability is key. An individual should have a right to his/ her structured data. This simple concept will undergird and allow all data management principles outlined above. Portability of structured health data will necessitate standardization, which in turn will allow interoperability (portability), automated consent and notice systems, federated storage, data transparency, control, access and so on. It is imperative that in the case of health data, this Commission require that health data is accessible to the individual in structured format. It is wholly insufficient to merely say that patients have a right to their data. In this day and age, meaningful access to data, should involve a right to their structured data. Its alternative – the pushing out of pdf files is akin to the troves of folders, papers and plastic bags that medical records in India are ferried in. Access to structured data, will allow the creation of countless third-party applications for patients, providers, researchers and policy makers. Within proper consent and data access laws in place, the interoperability permitted by such structured data will result in innumerable benefits to the individual, to society and to

science. The law may provide for an extended period of time for entities to become compliant with the provision of structured health data. India has already adopted several international standards for health data standardization and interoperability. The law must stimulate their implementation at scale.

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.

   For health data, preventing all algorithmic decisions may preclude advances in care delivery. Yet, given the vast potential for misuse, we recommend the following principles: Health data may not be used for any automated decisions about access to care, or access to finances for care. Health data may not be used for any automated decisions that are used for marketing products or services to individuals (with time, Indians may choose to allow notifications of products and services that are targeted to their health status – in case of certain diseases or lifestyles. However, the default should be "no." Opt-in consent should be required for marketing ventures. Health data may be used for other apps or services that make automated decisions, but with consent. For example, a travel app that recommends vaccines may need access to the patient's vaccine record, and will to know where she is traveling, to recommend vaccines and prophylactic medications (say, anti-malarials) every-time the person travels. These automated decisions become more "black-box" when they are recommending doctors, medications or lifestyle changes based on a host of determinants that the individual does not know they are accessing – for example GPS tracking, mobility tracking, credit card receipts (fast food consumption), etc. Such use may not be permitted, or may be highly restricted now, but the law should certainly allow for such provisions as digital literacy and quality of consent notifications improves with time.

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?

   See above

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

   Where personal data are processed for the purposes of direct marketing, the individual should have the right to object to such processing or profiling. The right should be made obvious. Consent should be explicitly sought. Health data should not be used for direct marketing without meaningful consent.

6. Are there any alternative views in relation to the above which have not been considered?

   Few matters of national security, public safety, or personal safety may trump the individual's right to restrict use of personal data. Such exemptions should be few and far between, and subject to audit and review.

10. Individual Participation Rights – 3: Right to be forgotten

The right to be forgotten has emerged as one of the most emotive issues in data protection law. The decision of the European Court of Justice in the Google Spain case and the repeated reference to this right in Puttaswamy necessitates a closer look at its contours, scope and exceptions, particularly as it raises several vexed questions relating to the interface between free speech, privacy and the right to know.

For a fuller discussion, see page 137 of the White Paper.

Questions

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

   Enshrined in Puttaswamy. For health data, this may be interpreted as the patient restricting portability and secondary use of certain parts of their health records. As discussed before the right to be forgotten may require a few exceptions in relation to health data: patients should not be able to withhold or alter parts of their record that may be relevant to the provider's safety. This is tricky. While the patient's general practitioner's own safety is not compromised by the patient's HIV status, for example, his surgeon ought to know his HIV status, in case of an accidental needle-stick injury in the operating room, for example.

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

   No – in case of health data, individuals should be able to restrict or delete processed health data. However, they may have to bear the cost involved. Laws may be required to ensure affordability and reasonableness of associated costs. Standard should be defined by data protection agency about the type of data to be forgotten.

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

   Yes, it is likely that an individual for her own safety may want her whole medical history deleted. Facts around her sexual history, childbirth or behavioral history may subject her to discrimination, or criminal arrest (for example, 377), and she may feel safer, if "forgotten", after her acute medical needs are met.

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

   Yes, in the case of health data, erasure.

5. 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)?

   Exceptions will be needed to ensure that no harm is done by withholding of data, and data withholding is in not in contravention of required policies. For example, a spouse may not be allowed to withhold information about an STD for his or her partner, especially if the disease is associated with high morbidity or mortality. This is often best

determined by other entities that regulate what diseases are reportable, to whom, by whom, and for what purposed. But these laws should be in tandem with the digital health data ecosystem and its consent, notice architecture.

REGULATION AND ENFORCEMENT

1. Enforcement Models

Once the substantive obligations of a data protection law are formalized, provisions regarding enforcement must be structured so as to ensure compliance with substantive provisions. Effective enforcement requires the consideration of certain aspects of institutional design and overall approach before we can develop and align individual elements of the framework. This may be in terms of the extent of burden placed on entities covered under such framework, the structure and functions of any enforcement agency, or the tools at its disposal. Enforcement models consist of: (i) 'command and control'; (ii) self-regulation; and (iii) co-regulation.

For a fuller discussion, see page 143 of the White Paper.

Questions

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

   Command and control regulatory mechanism will likely be an outdated mechanism with modern data processing technological advancement. Co-regulation is the desired approach with self-regulatory participation and government oversight.

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

   Yes, co-regulation seems to be a better approach as rule making or decisions on codes of conduct can be shared between the government and industry. It allows for innovation from the private sector to be combined with oversight and protections from the public sector.

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?

   Healthcare is best co-regulated.

2. Accountability and Enforcement Tools

Accountability:

A data protection law must reflect the principle of accountability. Accountability should not only be enforced for breach of data protection obligations through the adoption and implementation of standards by data controllers, but also in certain well-defined circumstances, it could be extended to hold data controllers liable for the harms that they cause to individuals without further proof of violation of any other obligation. The data protection law should appropriately identify such harms for which the data controller should be held liable in this manner.

For a fuller discussion, see page 147 of the White Paper.

Questions

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

   For health care, all data controllers should take appropriate measures to implement data protection principles, and must be in a position to demonstrate, when asked by a supervisory authority, that such measures have been adopted. This is standard practice in many regions around the world. Accountability, as a principle of data protection, has existed for some time and has found mention in various privacy laws around the world. It is imperative that health data protection law reflects the principle of accountability, especially since health data will almost always be processed, and the majority of it aggregated, anonymized and without consent. In the context of health data, the concept of harm should necessarily include denial of services.

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?

   Standards should be agreed upon jointly by controllers, learned intermediaries and the government. In case of health data, accountability may best be demonstrated by developing mechanisms that allow the tracking and audit of data, personal or otherwise.

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

   Yes.

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?

   Controllers should be allowed mechanisms of indemnity and contractual affixation of liability inter se.

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?

   Yes.

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?

   Yes, especially controllers of health data.

Enforcement Tools:

A number of regulatory tools and mechanisms may be simultaneously utilized to achieve different enforcement objectives such as flexibility and rigour in compliance. It needs to be determined which regulatory tools and mechanisms will find place in a data protection law for India.

A. Codes of Practice

For a fuller discussion, see page 157 of the White Paper.

Questions

1. What are your views on this?

   In healthcare, codes of practice have existed in both the clinical and research environments. The patient's Bill of Rights, Institutional Review Boards, HIPAA, occupational Health and Safety Regulations, etc. are some examples of existing codes of practice that should be integrated into any technical solution that seeks to address health data privacy.

2. 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?

   In the context of healthcare, include an interdisciplinary team of experts from computer science, data science, mobile technology, medicine, public health, finance and law, from India and abroad, from the private and public sector, from industry, academia, and government. Include consultations with patients from various demographics, including those with limited health literacy or digital literacy.

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

   A co-regulatory authority comprised of personnel from multiple disciplines related to medicine and healthcare, that include IT experts, policy makers and patients.

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.

For a fuller discussion, see page 161 of the White Paper.

Questions

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

   The law may require that individuals be notified of data breaches where there is a likelihood that they will suffer privacy harms as a result of such data breaches. · The law may also require that the data protection authority or any authority be notified

immediately on detention of data breaches. · Fixing too short a time period for individual notifications may be too onerous on smaller organizations and entities. This may prove to be counterproductive as well as an organization may not have the necessary information about the breach and its likely consequences. · The data protection authority may issue codes of practice which prescribe the formats for such notification

2. How should a personal data breach be defined?

   "Personal data breach" is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Personal data breaches can take multiple 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.

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

   The law may require that the data protection authority or any authority be notified immediately on detection of data breaches.

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

   Confidentiality breach: Where there is an unauthorized or accidental disclosure of, or access to, personal or sensitive health data · Integrity breach: Where there is an unauthorized or accidental alteration of personal or sensitive health data · Availability breach: Where there is an accidental or unauthorized loss of access to, or destruction of, personal or sensitive health data.

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

   Health data breaches to an individual should include as much information as possible because the availability of sensitive data could expose the individual to harm. Describe the type of data that was breached, the date, and the circumstances surrounding the breach (in language that the lay person would understand), recourse and remedy. Notification must be in a format that is accessible to the recipient and be language and literacy level appropriate.

C. Categorisation 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.

For a fuller discussion, see page 167 of the White Paper.

Questions

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

   It would be difficulty to categorize data controllers without first defining what constitutes health data. That being said, broad categories could include individual providers, hospitals, diagnostic facilities, pharmacies, insurance companies, equipment manufacturers, software providers, wearable devices and health apps. Such categorization will help attribute liability among health data controllers depending on the types of data they access and process.

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

   Yes, as described in the paper.

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

   It will be hard to rank harms caused by different data controllers in the health data ecosystem. For example, each of the entities above would have access to both personal and sensitive health data.

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

   See above

Registration

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

   Yes. Most controllers of health data ought to be registered. As health services expand, become decentralized and move from clinics to phones, wearables and apps, such registration will become challenging, but may still be necessitated to ensure that patient rights (privacy, participatory, portability, right to be forgotten, etc.) are not compromised.

Data Protection Impact Assessment

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

   DPIAs will be important for personal and sensitive health data. However, as technology advances, and depending on the route India takes, much of this work can be automated and hardwired into the design.

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

   DPIAs may be mandatory where processing involves the use of new technology at scale, or the likelihood of harm to individuals. In healthcare, scientists are used to submitting research proposals to ethics committees that, based on the likelihood of harm to individuals, will deem the proposal fit for exemption, expedited review or full review.

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?

   DPIAs should always be conducted by the data controller. Volume, potential for harm and sophistication of technology may warrant external review or government oversight.

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

   Transparency is key to building a successful health data ecosystem that is not cripples by command and control, and notice and consent paradigms. DPIA reports should be readily accessible, to promote accountability to the individual and the community.

Data Protection Audit

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

   It would be beneficial for the data protection law to provide for data protection audits in a regular manner for data controllers whose activities pose higher risks to the protection of personal data. A useful framework need not require the regulator to always carry out such audits itself and the law may provide for the registration of independent external auditing agencies. Audits may also be required when exemptions have been activated, to prevent abuse by the public or private sector.

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

   Yes, this may be determined by type of data, volume of data, harm risk and nature of technology involved.

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

   Compliance with prescribed norms.

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

   Third party (external person/agency)

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

   Yes.

Data Protection Officer

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

   The designation of a specific individual or officer by a data controller to facilitate compliance through monitoring and advising as well as to act as a point of contact with a data protection authority is a crucial element of data protection laws. These individuals are often called data protection officers (DPOs). It is relevant to note that in the present

Indian legal framework, a body corporate is required to designate a grievance officer for grievance redressal purposes with certain details of the same posted on the body corporate's website. Certain categories of data controllers (see above) may be mandated to maintain a DPO.

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?

   Yes.

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

   DPOs should be primarily responsible for accountability in the data controller's organization - accountability to the individuals whose data they process, and to the data protection authority, if one exists.

D. Data Protection Authority

The effective enforcement of data protection law may necessitate a separate, independent regulatory authority. Such an authority may discharge the following types of functions, powers and duties: (i) Monitoring, enforcement and investigation; (ii) Standard-setting; and (iii) Awareness generation.

For a fuller discussion, see page of the White Paper.

Questions

1. What are your views on the above?

   The law gives India citizens the right to privacy. Deposition of personal data with several public and private agencies puts an individual's privacy at a risk. This necessitates the creation of an independent data protection authority where individuals can seek guidance, direct queries and complaints in relation to data protection violation. Such an authority would ensure best practice protocols, and mitigate potential misuse of personal data by public and private authorities. To be consequential, the DPA may need to be an autonomous body, that has the power to monitor, regulate and censure both the private and public sector.

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

   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?

   No, the CIC is already overburdened. The DPA may require to be an independent autonomous body with a budget to support an interdisciplinary team of experts that are continuously reviewing various provisions of the data protection laws to keep them in sync with changing societal mores and evolving technologies.

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?

The DPA must be interdisciplinary and include representation from the major sectors it will regulate, including health.

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?

The estimated capacity of members and officials of a data protection authority would be at most of 1000. (Central Government Data protection authority: 11; State Govt. data protection authority: 29 X 11 = 319; A data protection officer at each district of the country: 640; Two Union territories - Delhi and Puducherry: 2 X 11 = 22; Total: 992; Therefore, maximum capacity may be set to 1000).

6. 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?

Yes, state level data protection authorities should be set up. Their jurisdiction should be restricted to the violation arisen from the said state / wherein data subject is a resident of the state. Constitution of such state level authorities should adopt the constitution of the model at the central government level.

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

The supervisory authority shall remain free from external influence, not take instructions from anyone, shall not undertake any action incompatible with their duties and not engage in any incompatible occupation during the term of their office. (Not different from the Election Commission of India). The supervisory authority must have its own staff which shall be subject to the exclusive direction of the members of the supervisory authority. Moreover, each Member State is required to ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has a separate public annual budget, which may be part of the overall state or national budget.

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

No. However, financial rewards may be considered for significant achievements in mitigating personal data infringements.

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

Data protection authority should ensure monitoring, enforcement and investigation of personal data infringements, create awareness, set standards and issue standards to public and private agencies dealing with personal data. Equally important, the DPA should ensure that the law is constantly evolving, in a timely manner, keeping up with emerging technologies. This nimble, adaptive structure will give India a competitive edge in the global market.

10. 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?

    In case of health data, standards are also best set by a participatory co-regulatory model.

3. Adjudication Process

Adjudication plays an integral role in enforcement of any law as it ascertains the rights and obligations of parties involved in a dispute and prescribes corrective actions and remedies. In the context of a data protection law, adjudication entails an assessment of whether and to. what extent data protection rights of an individual have been infringed by a data controller, the loss or damage suffered by the individual due to the said infringement, the remedies available to the individual as well as the penal consequences that the data controller may be liable for.

For a fuller discussion, see page 184 of the White Paper.

Questions

1. What are your views in relation to an adjudication process envisaged under a data protection law in India?

   Effectiveness of data protection authority can be ensured with distinct and defined adjudication process based on nature and impact of personal data infringement on the data subject. In this regard, the data protection authority should be given the power to adjudicate on disputes arising between an individual and a data controller in case of breach of any data protection obligation.

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

   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?

   An adjudicating officer should possess experience in the field of Information Technology/ Data Science and legal or judicial experience as may be prescribed by the Central Government (as followed in Section 46(3), IT Act). Ideally, in relation to health data, the officer (or a pair) must also possess domain expertise in medicine or public health.

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

   Yes.

5. 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.

Any individuals aggrieved by an order made by an adjudicating officer under the Act may prefer an appeal to Appellate Tribunal having jurisdiction in the matter. However, no appeal shall lie with the Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties (as followed in Section 51(1) and Section 51(2), IT Act).

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

   Implementation of digital mechanism, wherever possible, would make adjudication and redressal process convenient and faster. It must be noted that the parties involved, data subjects in particular, are adequately educated to handle these modes of communications.

7. 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?

   No. This will vary from sector to sector, and on the harm caused to individuals or communities. 5 crores, for example, may end up being a small figure in the context of data use violations committed by large corporations, and not necessarily and adequate deterrent.

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

   Yes.

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

   Yes, those with larger claims.

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

    Yes, if there is a prescribed cap.

11. Should class action suits be permitted?

    Yes.

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).

For a fuller discussion, see page 191 of the White Paper.

Questions

1. What are your views on the above?

   Our group did not reach consensus on which model would be best, with group members selecting one or more of each of the three.

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

   The type of violation for which civil penalty may be prescribed include failure to operate good policies, procedures and practices to protect personal information; nature of personal information involved; intentional or negligent character of the infringement; duration and extent of contravention; likelihood of substantial distress or damage, including bodily harm, discrimination, or violence; any relevant previous infringement by the data controller or data processor.

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?

   Strict liability of a data controller should 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?

   Our group did not reach consensus of which model would be best, with group members selecting one or more of each of the three.

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?

   Our group did not reach consensus of which model would be best, with group members selecting one or more of each of the three.

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?

   Worldwide turnover

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?

   Should be prescribed under law

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

   Yes.

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?

   The parameters to be considered for the quantum of civil penalty are failure to operate good policies, procedures and practices to protect personal information; nature of personal information involved; intentional or negligent character of the infringement; duration and extent of contravention; likelihood of substantial distress or damage, including injury to feelings or anxiety suffered by data subjects; any action taken by the data controller or data processor to mitigate the damage suffered by the data subjects; any relevant previous infringement by the data controller or data processor.

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?

    Yes. This will set as deterrence for other data controller agencies.

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.

For a fuller discussion, see page 197 of the White Paper.

Questions

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?

   Any "material or non-material" damage as a result of infringement 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?

   The factors or guidelines may be considered are failure to operate good policies, procedures and practices to protect personal information; nature of personal information involved; intentional or negligent character of the infringement; duration

and extent of contravention; likelihood of substantial distress or damage, including injury to feelings or anxiety suffered by data subjects; any action taken by the data controller or data processor to mitigate the damage suffered by the data subjects; any relevant previous infringement by the data controller or data processor.

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

   The mitigating circumstances to be considered may be the size of the entity, unintentional infringement, lack of harm to the individuals, and short duration of infringement before rectification, among others.

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?

   No. Compensation must be through an adjudicatory mechanism.

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.

For a fuller discussion, see page 201 of the White Paper.

Questions

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?

   Reckless disclosure, sales, offers to sell or unauthorized transfer of personal data to a third party may be considered as criminal offense. The degree of harm posed to individuals by such behavior may also be considered as a determinant of criminality.

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?

   Fine and / or imprisonment, if not in accordance with permissible sharing as prescribed by the law.

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

   Yes.

4. 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?

   Data protection law itself should set out all relevant offences in relation to which criminal liability may be imposed