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

A LENS ON CHILD PROTECTION

HARVARDFXB
CENTER FOR HEALTH AND HUMAN RIGHTS

AUTHORS

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

Amiya Bhatia
Doctoral Candidate, Harvard T.H. Chan School of Public Health

WITH REVIEWS AND CONTRIBUTIONS FROM

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

GENERAL COMMENT

Given the specificities of the Indian context, and in particular the erratic nature of infrastructure and energy provision, the lacunae in political accountability at many levels of governance and the vast social and economic inequalities that hamper effective accountability, care should be taken when citing US, EU and Australian practices as easily replicable models for contemporary India. The significant digital divide and the well-documented lacunae in policy implementation militate against over ambitious technological fixes to basic social problems. With these caveats in mind, we offer some comments in response to the questions posed by the White Paper.

RESPONSES TO CHAPTER 2: CHILD'S CONSENT

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

Adults and children should not be conflated in one single group of data subjects. Specific protections are necessary for children in the context of (1) consent; (2) notice; (3) services which process and/or sell children's personal data. Such protections should also apply to cases where the government collects data about children.

The protection of a child's personal data should be in line with the 1989 UN Convention of the Rights of the Child (CRC) and the 1948 Universal Declaration of Human Rights. Indeed, these rights should also apply "online": any act against a child which is illegal in the real world is illegal online. India has ratified the CRC and is therefore bound by its provisions. In particular, it is required to comply with the requirements of CRC Article 3(1) which provides: "In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration". For detailed and expert guidance on how to adhere to these obligations, UNICEF offers recommendations and good practices for how to protect children's data and ensure privacy.

The use of children's data for (1) sexual abuse and sexual exploitation including child pornography, (2) bullying and harassment, (3) advertising and marketing, (4) sale of children for labour exploitation, abusive adoption, marriage or other egregious practices is particularly concerning. Any acceptable data protection law should aim to protect children from these risks.

Additional considerations apply when children's biometric data are collected. To be sure, such data do have possible benefits for protecting children from harm. Facial recognition software could be used to detect and remove child sex abuse images from the internet, and biometric identification can be used to connect children to caregivers from whom they have been abusively or accidentally separated. However, the risks to children when identifiable data includes biometric information are more substantial. Undue pressure (a common occurrence given power imbalances between adults and children) exercised upon children can lead to privacy breaches and data interference, with potential knock on effects on protection from exploitation and access to social protection. These breaches can have spillover effects on family members and others in the child's extended social support circle.

In databases where the citizenship, caste, SC/ST/OBC status, or disability of a child are collected, stateless, disabled, or otherwise vulnerable children might find themselves

at particular risk of discriminatory targeting.

Penalties are required for the harmful use of children's personal data – including the sale of these data, their use online for child pornography, and their use to market harmful substances to children (e.g. cigarettes, drugs). Perpetrators of child abuse, including those producing and disseminating illegal content and child abuse material, those responsible for trafficking children for exploitation, and those engaged in recruiting them for child labour, must be tracked and sanctioned.

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

Given that approximately 1 in 3 Internet users is aged under 18, and that children require special protection, the data protection law should have a provision specifically tailored towards protecting children from targeted abuse and to ensuring firewalls than protect children's personal data. Children are vulnerable to abuse, cyber bullying, and to the adverse impacts of direct marketing activity. Adequate and specially targeted safeguards for children are thus imperative. Rigorously enforced and monitored penalties to address the use of child abuse material are also essential.

The data protection law should regulate (1) how children consent, (2) the methods used for age verification, (3) the storage of child data, (4) how the right to be forgotten applies to children.

The data protection law should prevent and penalize the production, use and dissemination of child abuse material, and the sale of children's data. There should also be penalties for products that enable hidden personal data collection in children's apps. The data protection law should be accompanied by policies and codes of conduct for businesses and the education sector on how to operationalize the protection of child data.

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?

The law should prescribe an age bar for consent, but since confirming consent and conducting age verification are both challenging, the law should not solely rely on consent to protect children. Instead it should ensure there are other safeguards to protect children.

Regarding an age bar, the U.S. Children's Online Privacy Protection Act (COPPA) recommends age 13, while the EU Genderal Data Protection Regulation (GDPR) recommends 16. The difference between these two age-bars is instructive. Each reflects cultural norms about maturity, agency and independence that are specific to the societies they apply to. The same reflection of cultural norms, assumptions and protections should be generated for India, after appropriate consultations. The specificities of a vast, religiously diverse and culturally multifaceted society such as India requires careful consideration of the appropriate age bar. Among constituencies that should be consulted in the process of determining the relevant bar are children, child rights organizations, teachers' and other expert bodies.

In addition to consent, there should also be a duty to inform children of their rights in relation to production, control and dissemination of data concerning them. This information should be available in clear and plain language, and in a concise, transparent,

intelligible and easily accessible form. It should be disseminated through educational and other appropriate institutions.

All websites and apps for children should be required to contain privacy protections in their default settings, and children's profiles should also be private by default.

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?

Data profiling of children should not be allowed for commercial profiling purposes. Such a restriction would be an important step towards protecting the rights of the child and address many of the challenges of consent and age verification. The process for establishing exceptions require appropriate consultation and accountability, along similar lines to those outlined in Point 3. above.

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?

Relying on the data controller to make this judgment will not sufficiently protect the child from harm. It will also be challenging for data controllers to assess capacity to provide consent on an individual basis. Additional safeguards, including those outlined above, are required.

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:

The data protection authority
The entity which collects the information
This can be obviated by seeking parental consent

No one dimensional test will be adequate to determine whether a child is capable of providing valid consent. Procedures need to be establish that generate standard operating procedures (SOPs) that take a multiplicity of factors including age, maturity, educational level and social context into account. The data protection authority or the entity which collects the information should be responsible for developing these SOPs in collaboration with agencies representing children themselves, and their rights and needs. Before implementation, any consent module should be tested, and the results should be assessed by experts, as a prelude to reformulation or amendment of the SOP.

Given (1) that many children and adolescents are more likely to understand and use the internet than their parents, (2) the challenges of seeking consent when parents might have low literacy, this test should not be obviated by seeking parental consent. Further, the responsibility for the data protection of children's data cannot solely fall to parents.

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

Parental consent cannot and should not be determinative of the validity of all consent obtained from children. It is clear, for example, that the child's age, maturity and educational level will have an impact on the appropriateness of a parental consent input. In our view, parental consent should never suffice for the establishment of valid child consent but the parents' views should be taken into account, in line with provisions set out CRC Art. 3(2) which provides: "States parties undertake to ensure the child such protection and care as is necessary for his or her well-being, taking into account the rights and duties of his or her parents, legal guardians, or other individuals legally responsible for him or her, and, to this end, shall take all appropriate legislative and administrative measures".

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

Yes, such a restriction could be effective, and such an approach should forbid the collection and use of child's data for sexual abuse, pornography, marketing, advertising and tracking purposes.

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?

General websites should not be exempt from having additional safeguards protecting the collection, use and disclosure of children's data. What is relevant is not the intended use of the website but the potential for harm, abuse and exploitation that child specific data carries with it, whoever the intended audience. Accordingly, all generators of internet based websites and databases should be required to conform to general standards that protect children from disclosure and potential exploitation of their data. Of course, there should be specific penalties against websites which sell or promote information about access to vulnerable children for exploitative purposes, including child labour, trafficking and child pornography.

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

Data controllers are responsible for implementing the protections set out in Point 9. above, whether children are using their services or adults are using services that provide access to information about children. They should be responsible for ongoing tracking to ensure up to date knowledge of the user base of their sites.

RESPONSES TO CHAPTER 10: RIGHT TO BE FORGOTTEN

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

The right to be forgotten must have a place in India's data protection law. Such a provision should also take the unique position of children into account. Children have a large amount of information about them online, leaving longer and deeper trails of electronic information than many adults do. Many Internet applications enable the sharing, reproduction and publication of images featuring children, including in cases where children are not informed, or did not consent. This has implications for children's privacy and autonomy, but its effects can also extend into adulthood as it may impact future employment, reputation, relationships and financial inclusion.

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

The right to be forgotten should not be restricted to personal data that individuals have given out themselves, but include data that was shared with or without an individual's consent or knowledge, and data which can harm an individual. This is particularly important to protect children's data.

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

Yes it does. Because children frequently first use the Internet when they are very young and immature, and because the data thus generated lasts indefinitely until deliberately removed, the imperative of a right to be forgotten is particularly critical for this constituency. Young children may have little or no recollection of data captured about them and subsequently displayed without their knowledge or consent.

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

There should be a child ombudsperson within the controller's office charged with specific child protection responsibilities. This person should establish a committee to review the procedure for justly and protectively implementing a "right to be forgotten" for children in relation to information about them captured on the internet.

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)?

The best interests of the child must be a primary consideration in this context and if it suggests that rights to freedom of expression or information would have a deleterious impact on the child then no exemption on the right to be forgotten should be granted. However, there may be fine cases where more specific consideration is necessary - these should be within the purview of the child data protection ombudsperson.

RESPONSE TO PART 4, CHAPTER 2: ACCOUNTABILITY AND ENFORCEMENT TOOLS

What are the subject matters for which codes of practice or conduct may be prepared?

Codes of practice or conduct will be essential for the education sector, and industry on how to protect children's data. A code of practice for how to protect the biometric data collected by Aadhaar may also be beneficial.

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?

The following stakeholders could be consulted to develop a code of practice concerning children: industry, mobile providers, internet providers, app developers, children and adolescents engaged in computer science clubs, competitions and other related activities, parents associations, teachers associations, paediatricians and child psychiatrists and psychotherapists, children and women's rights civil society organizations with expertise in trafficking, child violence and sexual abuse and pornography, the Ministries of Women and Children, of Education, of Labour, of Justice and Home Affairs, UNICEF.

Who should issue such codes of conduct or practice?

The government following the advice of a specialist committee chaired by the Ombudsperson for Data Protection with the Controller's office.

How should such codes of conduct or practice be enforced?

Codes of practice should be monitored and a complaints system should be in place so reports of violations of the data protection law can be investigated.

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

A graduated hierarchy of sanctions and penalties should be established, in consultation with specialist agencies charged with the protection of children's rights.