2019

FLAIR – FORUM FOR LEARNING AND ACTION WITH INOVATION AND RIGOUR

Ajay Kumar Sinha

Forum for Learning and Action with Innovation and Rigour

POLICY PAPER SERIES – DIGITAL MEDIA AND SOCIETY

NO. DMS-PP-2019-01

[PROTECTION OF RIGHTS OF INDIA'S CHILDREN IN A DIGITAL SOCIETY - A RIGHTS BASED FRAMEWORK]

Situation Analysis of Children's Rights in the age of Big Data and Artificial Intelligence and Recommendations for Legal and Systemic Provisions to Protect Children from Harm in a Digital World

DMS
DIGITAL MEDIA & SOCIETY

CONTENT **PAGE NO.**

I. DIGITAL IDENTITIES AND CHILDREN'S RIGHTS

On 12 September 2014, the Committee on the Rights of the Child devoted its twenty-first Day of General Discussion to "Digital Media and Children's Rights". The objective was to analyse the effects of children's engagement with social media and information and communications technologies (ICTs), in order to better understand the impact on and role of children's rights in this area, and develop rights-based strategies to maximize the online opportunities for children while protecting them from risks and possible harm without restricting any benefits. At the General Discussion on "Digital Media and Children's Rights", Prof. Sonia Livingstone, Department of Media and Communications, London School of Economics and Political Science, explained that children's lives increasingly have a direct online engagement component and that it is hard to draw the line between online and offline when discussing their lives. Yet, children's needs are rarely considered explicitly when formulating policies in this area. They tend to be ignored, left to parents or considered undemanding because children are supposedly "digital natives". At the same time, almost every day, we see reports in the media about the risks that children face online, such as Internet pornography or companies seeking new ways to profit from children.

At that meeting on General Discussion on "Digital Media and Children's Rights", Prof. Livingstone also emphasized that although the Convention on the Rights of the Child had been formulated in the pre-digital era, the rights enshrined therein remained as relevant as ever. She pointed out that the emphasis should be on the right to protection from harm, the right to provision to meet needs and the right to participation as an agent, or citizen. The task at hand was therefore to identify where, when and how the Internet reconfigured the conditions of harm, need and agency.

For the State and the Society to ensure children's rights in the digital age, there has to be a very clear understanding of the fast-changing, highly complex and transnational nature of socio-technological infrastructures and realization and acceptance of the fact that the Internet is largely blind to age, treating children and adults equally.

The tasks at hand are complex, and the solutions to the problems largely unknown. Like all ethical and philosophical conundrums, there are frameworks that provide some guidance, but rarely give specific

details of problems and solutions. The devil is in the details and the details need to be understood before we even begin to move forward. In this paper we have discussed about the challenges in the way of ensuring Children's Rights, in the age of Big Data and highly inadequate legal framework at the national and transnational levels, and pathways to deal with and overcome them.

Data collection, analysis and regulation in the digital age raise questions about both the realization and the protection of children's rights. The questions are whether traditional ethical frameworks guiding research in institutional settings and national legal and policy frameworks for data collection and consent from children are adequate and sufficient. It is important to understand that, a higher share of collection and analysis of big data is not carried out by research institutions, but by the aid of "machines" and "artificial intelligence" through "automation" processes and hence such big data are not bound by human subject protections. Furthermore, big data is collected by both public and private organizations, and is therefore subject to multiple and varying international and state-based interventions and standards. There is severe lack of guidance, and/or practical and effective solutions, to safely collect data directly or indirectly from or of children in a digital world and process them.

One of the most critical issues that relates to Big Data and Children is the impact on their digital identities over their life course. "The networked self is an amalgam of identities that are created across multiple online platforms, constituted via an array of social media tools"[1]. This digital identity is extremely dynamic and keeps changing and updating as the software platforms are constantly busy in the acquisition and processing of information (updates, photographs, additional information). We also observe that, an individual's/child's material online is often generated by other users and the written and visual images provided by others may have greater impact on an individual's/child's digital identity than by what they provided themselves[2]. Hence despite even the most careful formation and pruning of one's digital identity and adherence to safety and privacy protocols, the online networks can, and do, hold significant power over these identities. The most significant player in the construction of digital identity is the host of the social media services that collects and utilizes the personal data, more often than not for economic purposes. Within this context, the data that is collected from and of children may, at any uncertain point in the future, be utilized and analysed by indeterminate algorithms, for

[1] Papacharissi (2010)
[2] Helmond (2010)

indeterminate clients, to create digital identities or to perform any operation in the digital space, of which the individuals/children are unaware and have no control.

The digital identities are formed not just by the corporate third parties and social media services, but also various digital service providers (including government and private parties), who collect, share and/or sell private and personal data. These organizations can collect, process and retain a range of data including self-tracking data, data collected from the Internet of Things (IoT), administrative data and data required of children to access programmes targeted at them. There is always a possibility of the child and/or their parent losing control over their digital identity, as the number of collectors and processors of children's data grows. Then we also see the repurposing of data and application of various algorithms on the personal data of children and it can have significant impacts on their reputation, access and costs of services, education, employment opportunities and personal security.

These are a few of the areas where digital identities can and may affect life choices and importantly, the opportunities available to children. While the limits to management of digital identity holds true for adults as well as for children, the impacts on a child's development are subject to more uncertainty given the biological and cognitive changes that occur during the course of childhood and adolescence to early adulthood and the resultant formation of self-esteem, individuality and independence. Therefore, there is a need to understand the issues clearly before a preventive, protective and curative framework for safe usage of digital identities of children can be proposed.

The facts sifted from the cobweb of facts, fiction and stories are as follows:

(1) Protecting children from potential harm in the age of the Internet and digital media is more challenging in disadvantaged communities. Adult supervision is not always possible as they often lack knowledge, awareness, time, tools and inclination to supervise children's use of ICTs;
(2) Roles and responsibilities of different social actors, including the State, school, families and civil society, to ensure that children can enjoy their rights in the digital environment are important. There is a basic difference between adults and children regarding ICTs: while children "live" within a world of technology, adults just "use" technology, thereby still idealizing a world without technology, as they knew from their childhood. This difference in perception also leads to different views on opportunities and risks relating to the online world;

(3) There are no policies and provisions to ensure access to "technical knowledge" for parents, particularly from families in vulnerable situations, and comprise measures to strengthen parents in their child-rearing responsibilities in general;

(4) This generation of children have had their lives 'datafied' – their digital footprints have been captured over their entire life spans, and will continue to be;

(5) The information contained on the internet and held within big data sets is pervasive and has the potential to substantially influence the children's opportunities as well as their 'digital' and 'offline' identities, with significant implications for their life course;

(6) Provision, creation, ownership and utilisation of this data involves a complex chain of actors, with varying degrees of understanding of the implications, risks and potential mitigation strategies;

(7) We have not yet imagined future data applications and implications, especially in the light of "Big Data" and formation of "Digital Identity" and finally;

(8) Children's rights are enshrined in international and national legislation, and we have a duty of care to protect them and to respect and uphold their rights as their capacities evolve.

II. CHILDREN'S RIGHTS IN THE AGE OF BIG DATA

Big data is a new paradigm of data-driven decisions. Big data comprises of a variety of data types including text, imagery, and video. Different sources of such data types are mainstream news articles, social media platforms, images on Instagram, professional photographs, satellite imagery and aerial imagery captured by Unmanned Aerial Vehicles (UAVs), and videos from TV channels, YouTube, Vimeo and other channels. The quantity of data that is being generated is huge. Even a developing country like India is producing huge amounts of big data. Rapid ICT development and users' engagement with platforms like social media, micro blogging sites, among others enable unprecedented gathering, retention, and analysis of big data.

We need to understand that "Big Data" is not solely a technological phenomenon; it also has cultural and social dimensions relating to expectations of its applicability, robustness, accuracy and objectivity, across multiple domains – ranging from education to justice systems[3]. The big data is also not just about volume, but also the velocity and variety of data elements and sources. These large databases are collected, created and owned by both government and private stakeholders. Most of these huge

[3] Boyd and Crawford, 2012

datasets are either collected by government to provide welfare services but managed or stored by private stakeholders or collected by private technology corporations. For example, in India, Census of India, Stock Exchange, the Ministry of Rural Development for the Mahatma Gandhi National Rural Employment Guarantee (MGNREGA), Unique Identification Authority of India (UIDAI), Income Tax Department, among others hold huge datasets. Other programmes of Indian government like Smart Cities Mission, Central Monitoring System, Human DNA Profiling, and Digital India programme also collect and retain big data. Besides the government, non-state actors like telecom providers, online travel agencies, and online retail stores collect big data and use big data analytics to promote their businesses[4]. The analytics of data collected from social media, websites, mobile GPS, and more could help to address various socio-economic problems[5] and help in evolving effective solutions and measures[6].

Thus, big data is being considered as an extraordinary resource that could potentially offer unique opportunities for all, but at the same time also reveal sensitive information of individuals. Along with big data, metadata[7] also has the potential to reveal sensitive information about people's lives, political preferences, religion, sexual orientation, etc. Metadata can reveal information like the time at which a particular webpage was accessed, IP address, location, etc. There have been cases of governments collecting metadata[8]. The business model of many internet companies relies on the collection of metadata, in order to improve their services and to infer user-behaviour to further improve their products.

However, gathering, accessing, and using such data carry significant threats to fundamental freedoms and human rights. Both — big data and metadata have the potential to seriously threaten individuals' rights to keep their personal and sensitive information private and to have control over how their information is used. Though there are positive characteristics of big data and most of these big-data oriented programmes have a clearly laid down privacy policy, there is a lack of properly articulated access control mechanism and there are serious doubts over important issues such as data ownership owing to most projects involving public private partnership which involves private organisations collecting, processing, and retaining large amounts of data.

[4] Buddhadev Haldar, 2018
[5] Morrison, 2016
[6] Coulton, Goerge, Putnam-Hornstein & de Haan, 2015
[7] Data that gives description of data
[8] Metadata summarizes basic information about data, which can make finding and working with particular instances of data easier

Big Data also raises ethical issues relating to the increasingly separate and distinct processes and actors involved in the creation and collation of data sets, analysis and use; their varying degrees of knowledge and technical expertise; their divergent interests; and the frequent absence of peer reviews or audits of data and algorithms to determine the validity of both the data and the consequent findings – used to inform decision making and also formation of "Digital Identity". "Digital Identity" that may include – (a) Race, colour, religion, ethnicity, caste; (b) Political affiliations; (c) Religious or philosophical beliefs; (d) Financial data; (e) Health data (Physical and mental health including disability); (f) Biometric and genetic data, (g) Marital status and sexual orientation; (h) Sexual activities; (i) Criminal history; (j) Employment history; (k) Trade union membership, political party membership, etc; (l) Passwords and encryption keys. And this "Digital Identity" is in constant beta and is ever changing and evolving with or without human interference.

In the case of children there are a number of defining features of their lives that interact with each other to imply that data science needs to explicitly consider its ethical implications for children. The most obvious of these is the growing demand for and use of big data and the rapid development of technologies for its collection and analysis. This accumulation implies that more data will be collected on children over their lifetime than ever before. It also needs to be understood that the future use, applications and consequent impacts on their lives, is still largely unpredictable.

Within this framework of big data, we can understand not only the nature of big data and its function but also its implications and potential impacts on children. In the absence of broader and coherent ethical frameworks for data science governance, children will suffer the consequences the most and for the longest duration. The net impact on children will be determined by our capacity to negotiate with this complexity and vulnerability of children and to explore, understand and address potential risks and benefits for them.

For the children growing up in a digital age, the traditional ethical frameworks for research and data collection are definitely inadequate and uncertain and do not keep pace with the fast evolving technological challenges. This is more evident in situations of persistent data collected throughout the probable life course of the child and "digital footprints", and the consequent uncertainty of the impacts of self-rendered and externally imposed "digital identities" on the life-long consequences and life

choices of children. This uncertainty renders any assessment of potential harm and benefits in the 'best interest of the child' as required by Article 3 of the UNCRC extremely difficult due to: (a) Unknown future applications of data[9]; (b) Children's and parents' understanding of the implications and applications of their data with the attendant implications for self-management of their digital identities[10]; and (c) The insufficiency of traditional informed consent and assent processes, given the nature of the data collected from the Internet, as well as the frequent opacity of the ages of data providers. This opacity has implications also as it may impede the adoption of a more nuanced definition of childhood in line with the 'evolving capacities' of the child, identified in Article 5 of the UNCRC and the recently adopted Committee on the Rights of the Child General Comment No. 20 on the Implementation of the Rights of the Child in Adolescence. Approaches adopted to ensure the realization of the rights of adolescents should differ from those adopted for younger children; recognizing children's development and their increasing competencies, analytical capacities and agency and the implications of consent.

Big data also has the potential to undermine child participation by encouraging the use of data analytics and artificial intelligence rather than dialogue and engagement to ascertain perspectives, preferences, attitudes and competencies, which would be a direct contravention of Article 12 of the UNCRC.

III. LEGAL APPROACHES AND PROVISIONS FOR PROTECTION OF CHILDREN'S RIGHTS IN INDIA IN A DIGITAL SOCIETY

Rights-based approaches are necessary for safety and protection of children within all forms of data collection, analysis and evaluation involving human subjects or sensitive secondary data. This approach provides explicit guidelines for data collection and processing, which includes reflection on issues pertaining to data privacy, the rights of children to be consulted on issues which affect them, informed consent, security and confidentiality.

It is a fundamental principle of the rights based approach that the processes of formulation of laws, policies and guidelines need to listen to children. There is a need to look into children's understanding of privacy, their perspectives on how their data should be treated, who should have access, and what controls they would like. To begin with we should be laying the foundations and undertaking the

[9] Fossheim and Ingierd, 2015
[10] Blackwell and Gardiner, 2016

preparations for a future where the rights of children and the generations that follow them are respected, recognizing that no one knows yet what the future will look like. Therefore, there is a need also to institutionalize a process through which the pace of formulation and enforcement of legal and policy frameworks matches the pace of technological development. There is a requirement to develop frameworks that will guide institutional, national and international practices for online safety and protection of children throughout the entire data cycle, from collection through to destruction or removal.

Multiple approaches are required to ensure ethical practices and outcomes as there is no clear and linear relationship between data providers, collectors, analysts and users. Multiple solutions should be considered, at each stage of the data chain. Solutions to ensure the protection and participation of children will need to explicitly recognize and respond to the reality that research and data collection is no longer bound by the established protocols and operating procedures of the academic community; analysis may be undertaken by people who may not be child rights experts or trained researchers, familiar with the concept of ethical standards, and may not be bound by notions of the best interest of the child. This may bring the benefit of fresh perspectives, but also significant ethical challenges.

III.1 India's Personal Data Protection Bill

India has prepared a draft of its own Personal Data Protection Bill. Following last year's Supreme Court landmark decision to uphold privacy as a fundamental right in India's Constitution, the bill seeks comprehensive data protection for the world's second most populous country. The Personal Data Protection Bill, 2018[11], is now likely to be introduced in Parliament of India, after the General Elections in 2019. The Ministry of Electronics and IT (MeitY) has sent the draft of the Bill to the law ministry for vetting after making a few changes, according to the official. After the Justice BN Srikrishna Committee[12] submitted the draft Data Protection Bill in July last year, the MeitY opened another round of public consultation, which attracted almost 600 sets of feedback, including from the US government.

While working on its own Data Protection Bill has the advantage of the experience of the European Union in the creation of its General Data Protection Regulation and observation of the general anti-

[11] http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf
[12] http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf

regulatory philosophy of the United States. But the national opportunity for India is not to follow in any other society's footsteps. Rather, it has the technical knowledge and the social commitment to build a new pathway of its own that will be important as an example to others throughout humanity.

There has already been an extensive analysis of draft Personal Data Protection Bill of 2018. While the debate promises to continue till the Bill is introduced in the Parliament and passed, there is one aspect of the report and the Bill that deserves attention - data processing and the rights of children.

There is a need to understand that the purpose of the legislation is not to protect data, but to protect people. This simple shift of focus affects the details of drafting, for we are making a statute to protect persons, not to regulate the general data economy. It affects the scope of application, which must be as transnational as necessary to protect every person to whom digital services involving data collection or processing are offered, no matter where in the world the data actually is stored or how it is processed, aggregated or modified. Protecting people means concentrating attention on the harms that can flow from data collection and retention, and providing remedies against those harms. One of the architectural mistakes India should not copy from the European Union is the attempt to center the legislative design on *types* of data, rather than types of harm against which law should provide remedy.

III.2 Children and Personal Data Protection Bill - Recommendations

(a) Discussion and Recommendation on Child's Right to Participation and Minimum Age of Consent

Children are distinguished from adults by virtue of their vulnerability and hence have a unique position in any legal framework. It has also been observed that the lawmakers and, indeed, the whole society equate vulnerability with dependence, and completely discount children's autonomy and decision-making capacities by purporting to act on their behalf, and for their best interests.

The Personal Data Protection Bill defines a class of entities who operate commercial websites or online services directed at children or process large volumes of the personal data of children, as "Guardian Data Fiduciaries" and absolutely bar them from activities considered specifically harmful, such as profiling, tracking, behavioural monitoring, or targeted advertising. The Bill also requires "appropriate mechanisms for age verification and parental consent" for all other data processing of children.

The Personal Data Protection Bill defines a child as being under eighteen years of age, the highest age of children in all data protection laws thus far. COPPA in the United States protects children less than 13 years of age, China's Standard covers children under 14 years old while in Europe, GDPR-K covers those less than 16 years old. According to the India's Draft Data Protection Bill, any company that uses information from minors would need to do so in "a manner that protects and advances the rights and best interests of the child". That includes robust mechanisms for age verification and parental consent. In the accompanying white paper[13] to the bill, it says "the processing of personal data of children ought to be subject to greater protection than regular processing of data".

In the modern era, eighteen might be against the principle of "evolving capacities" of children as enshrined in the UNCRC. The Bill justifies it on the basis that the Indian legal system, and especially the Indian Contract Act, sets the age of majority as eighteen. The Bill appears to deny to legal minors any effective participation in decisions about how their data is to be processed. Even though the Indian Contract Act defines majority and thereby, the capacity to contract at eighteen does not preclude a Data Protection Bill from fixing a different age, especially since the kinds of instant contracts people enter into in the digital world are of a vastly different character than the contracts envisaged by a law enacted in 1872. There is a need to treat children with due respect and as partners in the processing of their data, instead of subjects at the altar of parental consent.

So far as Data Protection Law and the Age of Consent is concerned, the data protection law may create the following situation:

i. The age of consent at which data controller can exercise their rights against a data subject can be set at 18 years in accordance with Section 11 of the Indian Contract Act, 1872 and Section 3 of the Indian Majority Act, 1875. Minors below the age of 18 years should not be compelled to provide their data in accordance with the law of contract. However, the principle of "evolving capacities" as enshrined in the United Nations Convention on the Rights of the Child (UNCRC) need to be applied and children of various ages should be a participant in the process of giving an informed consent, If such consent is deemed beneficial for the child. Parental Consent in an informed manner should also be provisioned.

[13] http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf

ii. A section can be created in the data protection legislation to empower a data controller to require ratification by a parent or a legal guardian in matters involving sensitive personal data.

iii. For all other situations, the data protection law should not restrict the ability of a child to provide consent for any service or product that is beneficial for the child in accordance with the law of contract.

For exercising the rights of a child as a data subject, there needs to be no minimum age limit, as a child should not be prohibited from exercising his / her rights under the law if they are below a certain age. The purpose of the law should be protecting the rights and interests of the child, and not to be an impediment for the child.

Designating a minimum age at which a data subject would become competent to give consent would create an unnecessary complication in the law of contract wherein the minimum age of consent for entering into a valid and enforceable contract would differ for the purposes of data collection, processing, use, transfer, protection and other data-related activities, and for other purposes for which a person may legally enter into a contractual relationship. A provision should be made in law to clarify that a minor's rights cannot be violated by a data controller if the minor has provided their data through proper informed consent and the data collection and processing causes no harm to the child.

Rights of the Child to opt out of consent on attaining majority

Another omission from the Bill is the right of a child to opt out on attaining majority. If the basis of parental consent is that the parent stands in as a proxy for determining the child's best interests, then it stands to reason that at the point of majority, when the erstwhile child is now deemed to exercise her own right to self-determination, an individual have the right to review the decisions made on her behalf, and "opt out" if she feels that they were wrongly made. This could be resolved by granting an individual the right, on attaining majority, to be informed of the terms on which her personal data has been collected, alter or rescind the terms on consent, and require the destruction of all personal data related to her. But the issue of "Digital Footprint" being a permanent feature and phenomenon online requires the legal and technological fraternities to discuss and debate more on the issue and come up with a solution in consonance with rights of children.

(b) Discussion and Recommendation 2 - Categories of People to be drawn on the basis of types of Harms faced

We should be protecting not data but people, drawing its categories from the harms against which people should be made safe, and the remedies for failures of safety. It should not be primarily a legislation for the protection of data as a basis for industrial activity. Therefore:

- Data safety legislation should define the harms that people can suffer, against which the law's remedies are directed. Harms of disclosure, harms of unpermitted aggregation or use for impermissible inferences or discrimination, harms of facilitation of crime or civil wrong — all should be given specific definition and characterization.
- In general, the principle of safety is control: that people should know when data about them is being requested, how that data is being processed, that the results of aggregations and combinations of their data with others data are being returned to them, as well as being used by others.
- In addition to rules giving people control over their data, there should be rules of accountability and safe handling. Parties responsible for the management of personal data on a large scale should be required to give people real-time access to information about use and handling of their data: who has requested it, what was provided, what rules or agreements govern how it can be used downstream, and how long it can be retained there. Safe storage practices (concerning encryption to protect against accidental or criminal disclosure, concerning access by judicial process in India or abroad, requiring accountability for all disclosures including disclosures to government) should also be defined by regulation and updated by ongoing government administrative process.
- Remedies must be provided that give swift recourse for people whose data is harmfully disseminated or mishandled. Large-scale processors of information should be required to post bond or otherwise ensure prompt recourse.
- A primary goal of data safety regulation should be to inform people of their risks and available remedies. It is crucial that the law itself, as well as the subordinate legislation to which it gives rise be as simple as possible. Data protection legislation often is devised to hide the protective dimensions in amidst the complexity of data science. That must not happen here.
- Companies that operate websites or other online services directed at children, or process large volumes of personal data relating to children, should not be allowed to profile, track, monitor

behaviors of, or run targeted advertising on, children, nor should they be permitted to extract personal data that could cause significant harm to the child.

(c) Discussion and Recommendation 3 - Distinction between Data Controller and Data Processor

The distinction between data controller and data processor, as proposed in the Personal Data Protection Bill, 2018, needs to be done away with. The purpose of the data protection legislation is to protect people and not data. Since the primary purpose of the law is safety, the responsibility or liability of the entity handling/processing data should be based on the quantum of risk they create. Any entity that creates potential risk of data breaches/leaks therefore causing harm to the data subject should be subject to clear accountability.

The obligations bestowed upon the data controllers should be as follows:

a) Data Controllers must be able to demonstrate compliance with national privacy principles such as notice, choice and consent, collection limitation, purpose limitation, access and correction, disclosure of information, data security, openness and accountability;
b) Data Controllers must implement appropriate technical and organizational measures to ensure and to demonstrate that its processing activities, conform to, and are compliant with the requirements of the Act;
c) Data Controllers must have written agreements with data processors that state all the requirements and safeguards for processing in the Act;
d) Data Controllers must maintain records of processing and report breaches to the concerned authority;
e) Data Controllers must notify concerned individuals in case there is a data breach;
f) Data Controllers must ensure encryption of personal data;
g) Data Controllers must ensure on-going reviews of security measures;
h) Data Controllers must ensure redundancy and back-up facilities;
i) Data Controllers must ensure regular security testing; and
j) Data Controllers must ensure adherence to approved codes of conduct.

IV. SYSTEMIC AND LEGAL PROVISIONS FOR PROTECTION OF CHILDREN'S RIGHTS IN DIGITAL SOCIETY - RECOMMENDATIONS

India has the largest child population in the world. As per the 2011Census of India, there are 472 million children below the age of eighteen including 225 million girls. They constitute 39% of our population. Cybercrime is a global phenomenon with the criminals acting at a transnational level. Cyber space is also being misused for child abuse which is increasing day by day both online and offline.

Based on children's rights based framework, there is a need for bare minimum standard content requirements for raising public awareness. The information needs to be tailored for different audiences according to their profile (e.g., age, gender, location, and special circumstances), envisaged roles and expected responsibilities.

Ensuring accurate information through several channels that are commonly used by stakeholders, particularly children and young people, is critical for enabling responsible use of technology rather than control mechanisms, albeit selective supervision and oversight and guidance by concerned adults is desirable.

The chances of success of efforts to raise public awareness on any issue are increased if the environment within which the communicators and audiences are located is conducive. The messages need to connect with the audiences if they are to take action. The desired changes can however occur only when the audiences are able to act upon the acquired knowledge and skills.

As we move forward, to ensure safety and protection of children in Digital India, following steps needs to be taken:

(a) Discussion and Recommendation 1 – Data Protection Regulatory Board with Separate wing for Protection of Children

There is definite need for a Data Protection Regulatory Board that should have a separate wing specifically for Protection of Children. The primary goals for the Board should be to provide speedy

and judicious remedy to persons affected by violations of their data safety rights and issuing injunctions to halt / prevent violations.

The functions, duties and powers of the Data Protection Regulatory Board should include:

- Monitoring, enforcement and investigation of non-compliance, including the power to initiate suo-moto investigations;
- Advising central and state government departments, bodies, organizations, and others for compliance with the data protection law;
- Review of existing and upcoming legislations, rules and regulations for compliance with the data protection law, and recommending changes to the Parliament where necessary;
- Standard setting powers;
- Awareness generation and educational programs;
- Review the adequacy of data protection laws and practices in other countries for cross border transfer of data;
- Creating a blacklist of known bad actors in order to restrict transfer of data to the blacklisted entities and countries;
- Formulating guidelines for best practices in data protection;
- Formulating model codes of conduct and standard clauses to be adopted by data controllers;
- Creation and maintenance of an automated tool to draft simple standardized privacy policies in multiple languages by filling in a simple form asking questions such as “Do you sell personal data to third parties?”, “Which of these types of data do you collect: Name, Age, Date of Birth, Address, Gender, Phone number, [...]”. The form could be made with checkboxes. Fields that need to by typed in, such as name of the company or product, could be kept in English only. The form would need to be adapted by the authority based on feedback from its users, so the authority must have the power to decide the contents on the form;
- Conducting impact assessment of new legislations, rules and regulations, new technologies, methods of collecting data, and processing of certain data, amongst others.

(b) Discussion and Recommendation 2 - Data Protection Regulatory Board to be Independent

The data protection authority needs to be completely independent of government control, as the authority's primary job of data safety is likely to clash with other tasks performed by various parts of the government. It needs to be independent in a fashion similar to the way that the judiciary is independent from the executive and the way that the Election Commission is independent. Ideally, a constitutional amendment is required to create a fully independent data protection authority. It should be created in a manner that ensures that its functioning cannot be influenced by the ruling government or corporate interests. It should not be allowed to undertake any profit making business; neither should it be allowed to accept any donations. The appointment, duration of service and disqualification of its members should be independent of government influence. If the government or corporations are able to exert any influence over the data protection authority, then its primary task – protecting personal data – would be compromised. Other jurisdictions have recognized this possible conflict of interest, and have created an independent data protection authority.

Another reason to create a separate and independent body is that Article 45 (2) (b) of EU GDPR requires the European Commission to take into account the existence and functioning of an independent data protection authority for a country to pass the adequacy test. Without such a separate and independent body, India is unlikely to be considered adequate for the purposes of cross border transfer of data.

(c) Discussion and Recommendation 3 - Formulation and Application of Privacy Policies

Users face "consent fatigue" while reading and agreeing to privacy policies mainly because of complex privacy policies and having to give consent to many service providers who have fairly distinct policies. Layered notices can address this issue. There can be two layers of a privacy notice, the first layer may contain condensed form of the actual notice, while the second layer should delineate full text of the Notice.

In addition, adopting measures such as standardization, localization and recommendation can further simplify complex privacy policies:

i. **Standardization of Privacy Policies:** Data Protection Regulatory Board can design standard privacy policies including easily identifiable symbols which can be adopted by service providers. These symbols must be shown to the user in the first layer of notice. Child Friendly Standards of Privacy Policies should be developed for specific needs of Children to be safe and protected online.

ii. **Localization of Privacy Policies:** All the standard privacy policies should be localized and made available in more than one language to ensure that users can understand them. Localized notices can be made mandatory. This will help the service providers who adopt standard privacy policies incur less cost for localization and also promote participation from the service providers in standardizing and localizing. Notice should allow a user to select preferred language in a way that a user can understand the label for the language drop-down as "choose your preferred language". Second layer must be shown in the chosen language.

iii. **Recommendation of Privacy Policies:** Data Protection Regulatory Board can recommend a user the level of caution they need to exercise while giving consent to a service provider based on their privacy policy using something like grades "A – can trust; B – check the few items (show them using symbols) from privacy policy; C – Do not consent unless necessary; D – Consent with extreme caution, includes non-standard policies)". Data Protection Regulatory Board can also give grades to each standard privacy policy and the grade for a group of standard policies put together will be the lowest grade of the policies included. Any Privacy Policy which includes non-standard policies will be rated the lowest grade possible. This grade of recommendation must be shown to the user in the first layer.

(d) Discussion and Recommendation 4 - New Data Protection Legislation to override all Inconsistent Laws

The new data protection legislation should override all inconsistent laws, so as to ensure that the protections provided under the data protection legislation are given precedence over any possible breaches under older legislations. No older law should be allowed to be used for reducing the protections offered to personal or sensitive personal data. An exception to this overriding effect can be made where the protections offered in an inconsistent law not only meet the requirements

imposed under the new data protection law, but impose a requirement of an even higher standard than the data protection law. The data protection law should not, for example, prevent a requirement under a financial law to implement a higher minimum standard of encryption than that which is required under the data protection law. Lastly, the new data protection legislation should not override the Right to Information Act, 2005 (RTI Act). Section 11 of the RTI Act contains sufficient protections for third party data. No additional protection is required for the purposes of RTI, and therefore, no amendment is needed in the RTI Act. The provisions under the Juvenile Justice (Care and Protection of Children) Act, 2015 and Protection of Children against Sexual Offences Act, 2012 and IT Act, 2000 and the Indian Penal Code, 1860 that give protection to children need to be retained and strengthened under the Personal Data Protection Bill.

(e) Discussion and Recommendation 5 - Data Protection Law and Protection of Children's Personal Data

A provision is required in law to clarify that a data controller cannot violate the rights of a minor under the data protection law. The data protection authority should also have a power to start an educational program to teach minors about their rights. The report titled 'Growing Up Digital' by the Children's Commissioner for England, published in January 2017, notes that children are unaware of how the internet works and recommends that an educational program should be set up to train children to be 'digital citizens'. Such a program could contain training of the following rights as per the report:

i. The Right to Remove: To be able to curate your online presence through being able to easily remove what you yourself have put up.
ii. The Right to Know: To know who has access to your data, why and for what purposes.
iii. The Right to Safety and Support: To know where to turn for support when something online is distressing.
iv. The Right to Informed and Conscious Use: To know that the internet is 'sticky' and that you have the power to switch off.
v. The Right to Digital Literacy: To understand the purposes of the technology that you are using and to have the critical understanding and the skills to be a digital creator.

In order to protect the interests of minors any data gathered from a person that is known to the data controller to be a child should not be transferred to an entity unless the data controller can ensure that any rectification or deletion requested by the child would also be performed by all entities to whom the data has been transferred. In other words, situations where such intimation may prove to be impossible or involve disproportionate effort should be minimized for children.

(f) Discussion and Recommendation 6 - Publication and Dissemination

Data Protection Regulatory Board should run a platform which publishes these standards. This platform can be used by Data Protection Regulatory Board and other individual volunteers & volunteer organizations to design the same. Having a platform is essential for localizing in least amount of time. Data Protection Regulatory Board should release a notification asking individuals/organizations from all over India to volunteer for localizing the standard privacy policies to all official languages as translators (one who translates text) and moderators (who performs 1st level of review). The Board could work with Indian language communities that work in the area of language localisation. For messages to be relevant for children and young people, agencies need to design communication and information materials and employ channels of communication based on a nuanced understanding of their communication and behavioral patterns. The importance of privacy and confidentiality should be negotiated and integrated within all educational initiatives considering the preferred channels of information through peers by this age group and the apprehensions regarding curtailment of their use of available technologies by the adults.

(g) Mandatory Periodic Reporting to the United Nations Treaty Body (Committee on the Rights of Child)

The Committee on the Rights of the Child (CRC) is the body of independent experts that monitors implementation of the Convention on the Rights of the Child by its State parties. It also monitors implementation of two optional protocols to the Convention, on involvement of children in armed conflict and on sale of children, child prostitution and child pornography.

All States parties are obliged to submit regular reports to the Committee on how the rights are being

implemented. States must report initially two years after acceding to the Convention and then every five years. The Committee examines each report and addresses its concerns and recommendations to the State party in the form of concluding observations.

The Union of India should compulsorily report on its systems, mechanisms and implementation on safety and protection of its children in a digital society to the Committee on the Rights of the Child in its fifth and sixth (combined) periodic report, which is due in 2019.

The Civil Society in India, working on the issues of Child Online Protection should also submit an Alternate Report to the Committee on the Rights of the Child.

References

1. Being Safe Online, Guideline for raising awareness among children, parents, educators and general public, NCPCR
2. Blackwell, L., Gardiner, E., and S. Schoenebeck (2016) "Managing Expectations: Technology Tensions among Parents and Teens." In Proceedings of ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '16). San Francisco, CA. Feb 27-Mar 2, 2016.
3. Boyd D., and Crawford K. (2012) Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon. Information, Communication & Society [Internet].
4. Buddhadev Haldar, Privacy in the Age of Big Data, (2018)
5. Claire Seraine, India's data privacy bill to protect minors under 18 years old, the highest age coverage of all data protection regulations so far, Totally Awesome, 2018
6. Fossheim H., Ingierd H. Introductory remarks. In: Fossheim H., Ingierd H., editors. Internet Research Ethics [Internet]. Hellerup: Cappelen Damm Akademisk; 2015
7. Gabrielle Berman and Karry Albright, Children and the Data Cycle: Rights and Ethics in a Big Data World, Unicef, June 2017
8. Gautam Bhatia, India needs to acknowledge the gaps in data protection and rights of children, Hindustan Times, 10 August 2018
9. Helmond, A. (2010) Identity 2.0: Constructing Identity with Cultural Software,
10. Livingstone S., and E., Locatelli (2012) Ethical Dilemmas in Qualitative Research with Youth On/Offline, International Journal of Learning and Media. Spring; 4 (2): pp. 67-75.
11. Livingstone S., Carr J., and J. Byrne (2015) One in Three: Internet Governance and Children's Rights. Global Commission on Internet Governance Paper Series. Oct; No. 22.
12. Papacharissi, Z. (2010). A Private Sphere: Democracy in a digital age. Cambridge, UK: Polity.
13. Report of the 2014 Day of General Discussion, "Digital Media and Children's Rights", Committee on the Rights of the Child