# Right to Privacy in the Digital Age:
# Submissions to UN OHCHR Resolution 48/4

## May 2022

V | D H | Centre for Legal Policy
Better laws | better governance

# This submission is undertaken by the Vidhi Centre for Legal Policy, an independent think tank doing legal research to help make better laws.

# About the Centre for Applied Law & Tech Research

The Centre for Applied Law and Technology Research (ALTR) has been established within Vidhi to spearhead original, independent research on crucial issues emerging within the law and technology domain. The team was formally constituted in September 2020, comprising an interdisciplinary roster of researchers from both legal and social science backgrounds. The Centre's key objective is to conduct high quality research, as well as engaging with the main stakeholders to translate our academic work into actionable reforms. Our ongoing work focuses on three main areas: data privacy and governance; internet and cyberspace regulation; and governance of AI. In pursuit of its research and policy work, ALTR works with diverse stakeholders including the Ministry of Electronics and IT (Govt. of India), the Supreme Court of India, IIIT Delhi, IIT Kharagpur, NITI Aayog, Dept. of Transport (Govt. of NCT of Delhi), Govt. of Telangana, etc. among other stakeholders.

# The right to privacy in India
# Response to OHCHR call for inputs on Resolution 48/4
# Centre for Applied Law and Technology Research, Vidhi Centre for Legal Policy[1]

## Prefatory remarks

In recognition of the increasing and pervasive impact of emerging technologies, especially on individual capacities to exercise fundamental human rights, the UN Office of the High Commissioner for Human Rights (**OHCHR**) adopted resolution 48/4 (**Resolution**). Pursuant thereto, it has solicited inputs on different issues pertaining to the risks to an individual's right to privacy in this ever-advancing era of digitalisation.

The Centre for Applied Law & Technology Research (**ALTR**) is an interdisciplinary research team within Vidhi Centre for Legal Policy (**Vidhi**). We work by producing independent, high quality research evidence, and leveraging the same for aiding legislators and policymakers in India in drafting better informed laws and regulations. Our work has featured policy and legal research around data governance and protection, internet regulation, and AI ethics and governance of AI.

Responding to this call for inputs, we have prepared this document enunciating how the right to privacy is faring in India's push for enhanced digitisation and techno-centric solutions. The right to privacy has only recently been recognised as a constitutionally guaranteed fundamental right under Article 21 of the Indian Constitution (Right to life and personal liberty). The Indian Supreme Court passed a landmark judgement in 2017, overturning almost four decades of jurisprudence, to recognise the necessity of safeguarding informational privacy in the digital age. Since the ruling, the right to privacy has received significant attention in public discourse and from policymakers, with a seminal draft data protection bill (**PDP Bill**) being currently debated in the Indian Parliament. However, despite these progressive steps, in the absence of a definitive legislative framework, there are concerns stemming from an increasing alacrity for data processing and data intensive technologies.

In this context, the present document will delve into four prominent issues emerging from India - first, we will be discussing the challenges regarding children's privacy in India and how far the proposed PDP Bill will address these; second, we will discuss the limitations of notice-and-consent frameworks in the tech age, which have traditionally been used to safeguard individual privacy and informational autonomy; third we will discuss the risks of arbitrary use of facial recognition (**FRT**) by Indian law enforcement; and lastly, we will discuss targeted surveillance using emerging technologies.

[1] The authors of this note are Ameen Jauhar (team lead), Jai Vipra (senior resident fellow), Trishee Goyal, and Dhruv Somayajula (research fellows).

## I: Children's privacy and India's data protection regime

Children are placed in a more vulnerable position than adults when it comes to personal data processing due to several factors. First, the capacity of children is not as well developed to understand the long-term implications of their data processing. Further, at their developmental stage, they are often not able to discern deceptive practices deployed by data processors. Second, the volume of personal data processed of "digital children" is significantly different from that of adults. Their personal data is subject to a much longer period of collection as also more intrusive ways of collection, through increased adoption of applications such as Internet of Things, which collect data continuously. Third, given their developmental stage, personal data processing practices such as profiling and automated decision-making lead to significantly higher impairment of their autonomy and exercise of choice as compared to adults.

Given these concerns, jurisdictions often take the approach of endowing children with none or limited agency in matters of personal data processing. This is mostly done by providing for a certain age limit below which children would not be considered capable of providing consent for their personal data to be processed (**age of digital consent**). Instead, a data processor must seek parental consent to process children's personal data. However, the solution is not so straightforward. There are two levels of concerns with this approach, first, at the conceptual level of adopting an age-gating approach to data protection, and second, at the level of operationalising this. We have undertaken considerable research in this context, especially within India. In the following paragraphs, we explore these concerns in the context of the proposed data protection law in India.

The PDP Bill provides that parental consent would be required for processing personal data of children under the age of 18 years. To ensure this, data processors are required to put in place age verification mechanisms, to confirm the age of users before any processing of personal data takes place. Moreover, all personal data processing must be done keeping in mind the "best interests" of the child. Additionally, it provides for a class of data processors called "guardian data fiduciaries" which are prohibited from undertaking certain kinds of personal data processing such as profiling, tracking, using personal data for targeted advertisement, and any other profiling that may be harmful for children.[2]

### Challenges for the law

Several concerns stem from this proposed position of law. Arguably, the age of 18 is considered too high for digital consent. The proposed law provides for this age on the argument that in India, 18 is the general age of majority, and because consent to process data is provided under a contractual framework, it should be considered the age of digital consent. This reasoning is flawed. The Indian Supreme Court has held in *Puttaswamy (I)*, the right to informational privacy is a natural right inherent in an individual from the moment she is born.[3] Merely because it is generally exercised through contract is not reason enough to tie the age of digital consent with the age of

[2] Section 16, Personal Data Protection Bill, 2019.

[3] Para 25, Page 487 (Sapre J.), Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

majority, especially given the harms that stem from it. Setting a high age of digital consent, that is arguably impractical (given digital usage by teenagers and younger adolescents), can encourage children to lie about their ages, with parents often agreeing to such deception. This deception makes it difficult for data processors to provide age appropriate guidance to children for a safe experience and results in lesser protections for children' data. It could further lead online service providers to offer fewer products / services aimed at children, given the regulatory compliance costs of instituting age verification mechanisms for users under the age of 18. Also, children who are vulnerable, such as sexual minorities, or those in abusive situations will have even less opportunity to access support communities and reliable information online.

In India, these concerns are exacerbated given the social and gender disparities that exist in accessing the internet. Digital age of consent being pegged at 18 will lead to differential access to children, given what their parents' threat perception and experiences with the internet have been. Further, even within the same social class, parents' attitude towards teenage girls accessing the internet is starkly different from that towards boys. Additionally, this approach also doesn't take into account India's obligations under the United Nations Convention on the Rights of the Child (**UNCRC**).[4] The UNCRC requires states to recognise the "evolving capacity" of children rather than a singular age of digital consent.

Additionally, operationalisation of the age verification and parental consent mechanisms, is often a data maximalist one, which compromises privacy interests of parents and guardians. Data processors typically collect a myriad of data points from them to verify the information that they have provided. There is no consensus on either the duty of care on data processors (which would ascertain the amount / nature of information they would have to collect) or the way they are supposed to do so. Collection of such information could in turn could lead to privacy concerns. Other jurisdictions such as the United Kingdom, which were keen on adopting age verification measures in other areas such as access to pornographic material, have had to drop their plans given the practical difficulties.[5] For these reasons, it is preferable and recommended that India move from a paternalistic approach to one where data processors adopt a "child rights by design" approach obligating data processors to provide relevant information to children in a more accessible manner and making privacy enhancing design choices.

## II: Beyond notice-and-consent frameworks in the digital age

The past decade has seen a rise in applications based on emerging technologies such as the Internet of Things (**IoT**) and artificial intelligence (**AI**) models by government bodies and private entities. These applications cover a range of applications including law enforcement, travel, healthcare, finance, marketing, and home use. The use of AI and IoT, often jointly, involves massive amounts of personal data processing for both its training and operational lifecycle. The increasing

[4] Article 5, United Nations Conventions on the Rights of the Child.

[5] In 2019, UK abandoned its proposed nation wide age verification mechanism to access online pornography in the face of privacy concerns and demonstrations that the age verification mechanism could be easily sidestepped. These concerns remained despite considerable investment of time and money in developing these products.

government adoption of these technologies for carrying out state functions raises the need for a holistic framework that protects privacy in the digital age.

**Control and informed consent**

In *Puttaswamy I*, the Indian Supreme Court recognised that the right to informational privacy included the right to control the use, or processing, of one's personal information. Meaningful consent is recognised as a central facet of autonomy and the right to informational privacy. This consent, (i.e., informational autonomy), is currently realised through the notice-and-consent framework. An individual is provided a privacy policy or certain terms and conditions explaining the processing of their personal data, and thus actively consents to personal data being processed. This allows an individual to make an informed choice.

However, obtaining an informed consent from a person is not sufficient towards ensuring informational autonomy. The widely used framework of notice-and-consent is inadequate in many aspects. The binary choice offered through standard form contracts, informational asymmetry, consent fatigue and dark patterns weaken the prospects of meaningful consent.

**Conventional 'notice-and-consent' inadequate to deal with emerging technology**

The growing adoption of AI and IoT systems is extensively reliant on collection and processing of personal data. These operations raise unique concerns regarding a data principal's autonomy over their personal data. However, the ubiquity of sensors and the person-agnostic manner of processing require data principals to exercise control beyond mere consent boxes. Emerging technologies require a nuanced take on informational privacy that extends throughout the period of processing personal data. The use of IoT devices at homes include wearable devices and smart home assistants that process data round-the-clock, and do not limit their operations based on individual consent. On a larger scale, plans to develop *smart cities* envision the deployment of IoT technology which aims for greater accuracy and efficiency through constant data processing. All these instances demonstrate the futility of traditional notice and consent frameworks which either seem redundant checkboxes, or in many instances have become a "take it or leave it" form of standardised contract. The fact that most services collect and process data far beyond what is necessary, contravenes data minimisation, and compels an individual to part with her personal data to continue enjoying day-to-day facilities and conveniences. The PDP Bill proposes to some extent, to check this by introducing measures to balance information asymmetry between data principals and data fiduciaries, as well as put in place redressal mechanisms for violations.

**State exemptions to privacy protections**

Notice and consent provisions become even more questionable when the entity processing personal data is sanctioned to do so by the government in India. With respect to the state processing personal data, the PDP Bill is considerably feeble, giving sweeping exemptions to governments and their agencies. The current version only requires the reasons to be recorded in writing, upon which the central government may exempt any agency from any or all parts of this law. In this regard, the Joint Parliamentary Committee Report on the PDP Bill has recommended

that the alternative procedures followed by the exempted agency must be just, fair, reasonable and proportionate in nature.

The scope of these potential exemptions raises concerns, particularly in light of the deployment of various emerging technology solutions by the central government in recent years. In addition to these, there are at least seventy-five instances where emerging technology has been deployed within India, with at least nineteen projects being launched by the central and state governments.

| S. No. | Ministry | Type of emerging technology | Name of project | Purpose |
|---|---|---|---|---|
| 1. | Ministry of Civil Aviation | FRT | Digi Yatra | Authentication: increasing ease of access to airports |
| 2. | UIDAI, Ministry of Electronics and Information Technology (MEITY) | FRT | Authentication Based Facial Recognition | Authentication: ease of authentication for Aadhar card |
| 3. | UIDAI, MEITY | FRT | Authentication Based Facial Recognition | Authentication- biometric authentication of Covid-19 vaccine recipients |
| 4. | Central Board for Secondary Education | FRT | Face Matching Technology | Educational- Identity authentication to access academic documents |
| 5. | MEITY | Conversational AI chatbot | Intelligent Virtual Assistant | Used in the MyGov Corona Helpdesk to interact with citizens having doubts |
| 6. | Jal Shakti Ministry | Internet of Things | Jal Jeevan Mission monitoring system | Used in monitoring implementation of Jal Jeevan Mission |
| 7. | NHAI, Ministry of Road Transport and Highways of India | Location tracking AI | Attendance Monitoring System | Real-time tracking of employees to ensure attendance |

The increased deployment of these emerging technologies by the central government raises concerns over the exemptions provided within the PDP Bill. As can be seen above, the foregoing AI-based programs involve processing of personal data as part of their functioning. Additionally, these provisions create an incentive for agencies to claim broad exemptions for a future purpose, with central government agencies such as the UIDAI and the Income Tax Department already

claiming exemptions prior to the bill being finalised. An individual having no awareness of the safeguards enjoyed by their personal data in an exempted agency does not retain means to ensure informational privacy. Even if an agency receives full exemption from the law, the wisdom or benefit of these exemptions for obligations such as reporting data breaches or maintaining security standards is not clear at this stage.

### III: FRT deployment by Indian law enforcement agencies

A growing number of local law enforcement agencies across India are deploying some form of facial recognition system within their territories. This usage is presently happening exclusively through executive action of the states, and in the absence of a legislative framework, or regulatory oversight. India, in its strategy document on the use of AI, has geared itself towards a society responsibly and safely using AI systems. This entails an adherence to our constitutional ethos, or *constitutional morality* which requires an unequivocal enforcement of rights and principles enshrined in the Indian Constitution.

With the use of FRT in the current arbitrary and unregulated manner by law enforcement agencies, this commitment to a responsible and safe usage of AI is endangered. In fact, in December 2021, the State of Telangana witnessed its first constitutional challenge to the state government's continued use of FRT systems in a myriad of functions.

It is pertinent to mention that FRT, like other algorithmic tools, demonstrates efficiency gains that can aid in surveillance and monitoring and law enforcement necessary for maintaining public order, and preserving national security. However, Indian law is presently unequipped to address executive overreach in technocentric policing, especially with emerging technologies like AI, and there are real risks to due process and the rule of law within India.

The risks predominantly can be categorised into privacy-oriented risks, design flaws, due process violations, and excessive delegation of core state functions. In terms of privacy, India is still in a legislative limbo working towards enacting its PDP Bill. However, even if the draft legislation were to be enacted in its current form, it affords sweeping exemptions where the state or its agencies are responsible for data collection and processing. Besides, an argument is to be made that surveillance reform requires a separate legislation as it entails issues above and beyond informational privacy.

Due process is also at risk in the current environment of unbridled use of FRT by local police. Indian procedural laws (like the Criminal Procedure Code and the Indian Evidence Act), are unacquainted to the use of algorithmic and predictive tools, both in investigation and trial. This absence of the law is seriously likely to impinge procedural and substantive due process in the event such evidence is actually used for charging and convicting an individual. It further leaves a potential accused without clear legal safeguards and remedies to assail such evidence in the course of her trial.

Beyond legal considerations, there are ethical risks in the unchecked use of FRT in Indian law enforcement. There is significant research evidence which indicates the basic design flaws of underlying algorithms driving FRT across the globe, with recorded instances of false positives which have driven a vocal opposition to the use of FRT in sensitive ecosystems. A misidentification of individuals in the context of the criminal justice system and law enforcement certainly imperils individual freedom and liberty, potentially threatening concerned persons with dire consequences including incarceration. In addition to accuracy concerns, there is the challenge of transparency and accountability (especially state liability) for any detrimental impacts emerging from the use of FRT. Apart from invoking the writ jurisdiction of a constitutional court, it is unclear what mechanisms, if any, will be available to citizens in India that face the growing onslaught of predictive policing.

Lastly, there is are concerns around how embedded private corporations are within the FRT ecosystem and the true extent of their participation in operationalising state surveillance apparatuses. Particularly, in terms of privacy, there is a risk of how private corporations and start-ups are sourcing the large swathes of visual data that is necessary for designing any FRT system. In the absence of a defined data protection legislation, effective monitoring of such an ecosystem is nearly impossible. The involvement of the private sector in providing FRT capabilities to the state is often shrouded in secrecy, with requests for information on procurement processes being denied or evaded by the police. There is no transparency in terms of the accuracy rates or other accountability measures undertaken by the private provider.

Also, due to the general lack of public information around procurement processes for FRT by law enforcement agencies, it is a concern that vital state functions may inadvertently be delegated to a private entity. The function of surveillance is a sovereign power and its exercise even for the state is exceptional. In no circumstances is such a function liable for delegation. Nonetheless, procurement of technologies often includes not only the design and development, but also operationalising and backend support in implementation. In the case of Indian law enforcement, this could arguably lead to a situation where a private entity ends up indirectly running an FRT system, and thus performing the actual act of surveillance, in a complete legislative and regulatory vacuum. Such a scenario is dangerous and highly disconcerting not only from a constitutional standpoint, but also from the perspective of a potential omnipresent private organisation driving state surveillance.

## IV. Targeted surveillance

Targeted surveillance refers to the subjection of specific persons or groups of people to surveillance. While governments may engage in targeted surveillance for legitimate purposes including public safety, often governments target dissidents, political opponents, journalists, whistle-blowers, etc. with surveillance, outside legitimate and legal bounds. Digital technologies have made targeted surveillance easier, with the ability of states and others to track people without leaving much trace of interception.

In the Indian law enforcement context, we have seen that FRT can be used to exacerbate police and societal biases, and target already marginalised sections of society. Our work in the context of policing in Delhi shows that the introduction of new surveillance technology to a law enforcement system with its own biases can exacerbate those biases. We found that due to the uneven distribution of police stations across the city, combined with existing biases, Muslim areas in Delhi would be more likely to be subjected to FRT (and its errors). This would constitute a disproportionate burden of FRT on Muslims in Delhi, a city which is segregated on the lines of class, caste and religion.

The use of new technology in policing is not limited to FRT. Mapping technology, data analytics, and other technology is often used for "predictive policing", which aims to target certain geographical areas or groups of people ostensibly "prone to crime". There is extensive research to show that such labelling of areas or communities as crime-prone is counterproductive, and leads to victimisation of marginalised people. In India, this targeting has been explicit even before the intervention of new technology. Certain tribes are designated "criminal tribes", and a list of "habitual offenders" is maintained by the police, allowing them to bypass due process for certain people.

Smartphone-based communication too can be intercepted with sophisticated malware that sometimes can be installed remotely without any action on the subject's part. Pegasus is one such malware produced and marketed by Israeli organisation NSO Group. Like other countries in the world, Pegasus was used to target journalists and opposition figures in India as well. Such tracking is deeply invasive, as it gives access to all communication, location, pictures, and other behavioural data. All these practices of targeted surveillance can have grave consequences due to the use of new technologies in strengthening them.

*******