CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY DELHI

RESPONSE TO CALL FOR INPUTS FOR THE REPORT ON 'THE RIGHT TO PRIVACY IN THE DIGITAL AGE'[1]

The Centre for Communication Governance is an academic research centre within the National Law University Delhi and is dedicated to working on information law and policy in India. It seeks to embed human rights and good governance within communication, information and technology law and policy and advance digital rights in India through rigorous academic research, policy input and capacity building. We thank the Office of the United Nations High Commissioner for Human Rights for inviting inputs on 'The Right to Privacy in the Digital Age' for the preparation of a thematic report. Our response to the call for inputs is below.

---

[1] *Authored by Jhalak M. Kakkar and Nidhi Singh with research inputs from Shashank Mohan, and edits by Sharngan Aravindakshan and research assistance by Anushka Pandey. This Response draws from our previous policy input provided to the NITI Aayog, the Indian government think tank, on the Working Document: Towards Responsible AI for All and to the AI Standardisation Committee of the Indian Department of Telecommunications (DoT) Discussion Paper on 'Indian Artificial Intelligence Stack'.* Comments to The Niti Aayog on the Working Document: Towards Responsible #AIForAll, Centre For Communication Governance At National Law University Delhi (2020), *available at* <https://ccgdelhi.org/wp-content/uploads/2020/08/CCG-NLU-Comments-to-NITI-Aayog-on-the-Towards-Responsible-AI-for-All-Document.pdf>; Comments to The Department of Telecom on the Discussion Paper on The Framework of An Indian Artificial Intelligence Stack, Centre for Communication Governance at National Law University Delhi (2020), *available at* <https://ccgdelhi.org/wp-content/uploads/2020/10/CCG-NLU-Comments-to-DoT-on-the-Discussion-Paper-on-Indian-AI-Stack.pdf>.

I. RIGHT TO PRIVACY IN THE DIGITAL AGE: IMPACT OF ARTIFICIAL INTELLIGENCE

The adoption of Artificial Intelligence (AI) and Machine Learning (ML) technology has the potential to provide numerous benefits to society. However, there are also several potential harms and unintended risks which may arise, if the technology is not assessed adequately for its alignment with international norms and national constitutional principles.[2] Depending upon the nature and scope of the deployment of an AI system, its potential risks can include discrimination against vulnerable and marginalised communities, and material harms such as the negative impact on the health and safety of individuals. Risks may also include violation of the fundamental rights to equality, privacy, freedom of assembly and association, and freedom of speech and expression. In this response, we discuss the privacy and related concerns that arise from the deployment of AI systems in the Indian context and some of the legislative and policy developments to regulate AI in India.

The deployment of various AI systems has raised concerns about their potential negative impact on constitutional values enshrined in the Indian Constitution.[3] In particular, the adoption of AI principles would have to strictly comply with the standards of anti-discrimination, privacy, the right to freedom of speech and expression, the right to assemble peaceably and the right to freedom of association as provided for in Part III of the Indian Constitution[4] and interpreted by the Supreme Court of India. For instance, the right to privacy has been interpreted by the Supreme Court of India in the case of *Justice K.S. Puttaswamy vs. Union of India* to broadly include autonomy, choice, and control in the context of informational privacy.[5]

---

[2] Comments to The Department of Telecom on the Discussion Paper on The Framework of An Indian Artificial Intelligence Stack, Centre for Communication Governance at National Law University Delhi (2020), *available at* <https://ccgdelhi.org/wp-content/uploads/2020/10/CCG-NLU-Comments-to-DoT-on-the-Discussion-Paper-on-Indian-AI-Stack.pdf>

[3] Comments to The Niti Aayog on the Working Document: Towards Responsible #AIForAll, Centre For Communication Governance At National Law University Delhi (2020), *available at* <https://ccgdelhi.org/wp-content/uploads/2020/08/CCG-NLU-Comments-to-NITI-Aayog-on-the-Towards-Responsible-AI-for-All-Document.pdf>

[4] Part III, Constitution of India, 1950

[5] *Justice K.S Puttaswamy (Retd.) v. Union of India*, (2017) 6 MLJ 267; (2017) 10 SCC 1, *available at* <https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors>

II. SPECIFIC IMPACT OF ARTIFICIAL INTELLIGENCE ON THE RIGHT TO PRIVACY

Given the diversity of AI systems, the privacy risks which they pose to individuals, and society as a whole are also varied. These may be broadly related to:[6]

i. Data protection and privacy: There are privacy implications around the use of data by AI systems and data protection considerations that arise from this use. There are two broad aspects to think about in terms of the privacy implications from the use of data by AI systems. *Firstly*, AI systems must comply with the legal frameworks for data protection; however, there are concerns around whether existing data protection frameworks can adequately address the privacy and data protection concerns raised by the deployment of AI systems. *Secondly,* given that AI systems can be used to re-identify anonymised data, the mere anonymisation of data for the training of AI systems may not provide adequate levels of protection for the privacy of an individual.[7]

   a. *Data protection legal frameworks:* ML and AI technologies have existed for decades; however, it was the explosion in the availability of data, which accounts for the advancement of AI technologies in recent years.[8] ML and AI systems depend upon data for their training. The application of existing data protection frameworks to the use of data by AI systems may raise challenges[9] and existing data protection frameworks may need to evolve to adequately address the privacy and data protection concerns that arise from the deployment of AI systems.

---

[6] Jhalak M. Kakkar and Nidhi Singh, "Building an AI governance framework for India, Part III", *available at* <https://ccgnludelhi.wordpress.com/2020/10/30/building-an-ai-governance-framework-for-india-part-iii/>

[7] Linnet Taylor, Luciano Floridi, and Bart van der Sloot, 'Introduction: A New Perspective on Privacy' in Linnet Taylor, Luciano Floridi, and Bart van der Sloot (eds), Group Privacy: New Challenges of Data Technologies (Philosophical Studies Series, Vol. 126, Springer, Oxford 2017)

[8] Bernard Marr, 'Why AI Would Be Nothing Without Big Data', (*Forbes*, 2017), *available at* <https://www.forbes.com/sites/bernardmarr/2017/06/09/why-ai-would-be-nothing-without-big-data/?sh=12db9dc44f6d>

[9] Big Data Value Association, *Data Protection in the Era of Artificial Intelligence*, (2019) *available at* <https://www.bdva.eu/sites/default/files/Data%20protection%20in%20the%20era%20of%20big%20data%20for%20artificial%20intelligence_BDVA_FINAL.pdf>

b. *Use of AI to re-identify anonymised data:* AI applications can be used to re-identify anonymised personal data.[10] To safeguard the privacy of individuals, datasets composed of the personal data of individuals are often anonymised through a de-identification and sampling process, before they are shared for the purposes of training AI systems. However, current technology makes it possible for AI systems to reverse this process of anonymisation to re-identify people, having significant privacy implications for an individual's personal data. International and domestic data protection and AI regulation frameworks need to adequately address these concerns.

ii. Impact on society: The use of AI systems raises broader privacy considerations that arise at a societal level due to the deployment and use of AI trained on the data of individuals, including systems for surveillance such as facial recognition systems, psychological profiling, and the use of data to engineer and manipulate public opinion. Based on a risk assessment of the impact of these AI systems on human rights, these systems need to be appropriately regulated through international norms and domestic legislation.

Besides privacy concerns, deployment and use of AI systems raise concerns of discrimination and bias. AI systems are trained on existing datasets, which tend to be historically biased, unequal and discriminatory.[11] Bias can creep into AI systems in several ways, such as using biased training datasets or using flawed sampling which over or under represents a particular minority.[12] Given that AI systems make decisions based on their training on existing datasets, we have to be cognizant of the propensity for historical bias and discrimination getting imported into AI systems. Unless we attempt to tackle this challenge, due to the nature of AI technology and its potential for widespread impact, such discrimination will not only get further embedded in society

---

[10] Rocher, L., Hendrickx, J.M. & de Montjoye, YA, 'Estimating the success of re-identifications in incomplete datasets using generative models', (2019)10**,** 3069 *Nat Commun, available at* <https://doi.org/10.1038/s41467-019-10933-3>

[11] Mehrabi et al., 'A survey on bias and fairness in Machine Learning', (Sep, 2019) *available at* < https://arxiv.org/pdf/1908.09635.pdf>

[12] James Manyika, Jake Silberg, and Brittany Presten, 'What Do We Do About the Biases in AI?', (*Harvard Business Review*, 2019), *available at* < https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai>

but also be severely exacerbated.[13] Given this, AI systems can have a disproportionate impact and consequences on marginalised and vulnerable communities, particularly in developing countries such as India. Additionally, marginalised and vulnerable communities have traditionally been at the margins of data collection and digital inclusion. Through appropriate regulatory and governance frameworks, we need to ensure that the deployment of AI systems in spaces such as fintech and health do not end up further alienating and marginalising these communities.[14]

Around the issue of bias, the "National Strategy for Artificial Intelligence" ("National Strategy")[15] discusses that bias is inherent in current datasets and that there is potential for such biases to get reinforced through the use of AI systems. The National Strategy suggests that fairer results can be achieved by identifying in-built biases, assessing their impact and finding strategies to reduce the bias in the datasets.[16] While such an acknowledgement of the need to find strategies to reduce bias in datasets are appreciable in their efforts to rectify the situation and yield fairer outcomes, we need to remain cognizant of the fact that these datasets are biased because they arise from a biased, unequal and discriminatory world.[17] Hence, there needs to be an appropriate risk-based assessment mechanism embedded in the AI regulatory framework to ensure the use and deployment of AI systems in consonance with human rights.

The effective regulation and governance of the use and deployment of AI technology must be cognizant of the fact that AI systems are socio-technical systems that reflect the world around us and embed the biases, inequality and discrimination inherent in society, with Indian society having many different kinds of bias such as gender discrimination, caste discrimination and economic inequality. This broader Indian social context must be considered while designing AI systems and creating regulatory

---

[13] Virginia Eubanks, *Automating Inequality: How High-tech Tools Profile, Police, and Punish the Poor* (St Martin's Press 2018)

[14] Jhalak M. Kakkar and Nidhi Singh, "Building an AI governance framework for India, Part II", *available at* <https://ccgnludelhi.wordpress.com/2020/10/09/building-an-ai-governance-framework-for-india-part-ii/>

[15] NITI Aayog, *National Strategy for Artificial Intelligence* (June 2018), *available at* <https://niti.gov.in/sites/default/files/2019-01/NationalStrategy-for-AI-Discussion-Paper.pdf>

[16] Ibid 85

[17] Comments to The Niti Aayog on the Working Document: Towards Responsible #AIForAll, s*upra* note 3.

frameworks to govern their deployment. The use and deployment of AI systems need to be balanced with their impact on an individual's right to freedom of speech and expression, privacy and equality.

III. EVOLVING LEGISLATIVE AND REGULATORY FRAMEWORKS IN INDIA

Regulatory standards and processes need to be developed at the international level as well as in India to ensure the safe use and deployment of AI systems. Many AI systems are being developed in developed countries and are being deployed in developing countries, raising concerns around whether they have been adequately assessed for safe deployment in a completely different context.[18] Additionally, India's Working Document Towards Responsible AI for All ("Working Document"), prepared by the NITI Aayog envisages that India can potentially be an AI Garage for 40% of the world - developing AI solutions in India which can then be deployed in other emerging economies.[19] Special focus should be placed on developing international norms and domestic regulation to enable the safe use and deployment of AI systems that have been developed in contexts that are distinct from the ones in which they will be deployed.

The Constitution of India provides fundamental rights protecting an individual's rights to equality,[20] privacy[21] and freedom of speech and expression[22] (among others) and specifically protects individuals against various forms of discrimination arising from India's historical and cultural context. The use of AI systems can infringe several of these fundamental rights enshrined in the Indian Constitution. Hence, as countries like India design a regulatory framework to govern the adoption and deployment of AI systems, it is important to keep the following in focus:[23]

i. Heightened threshold of responsibility for government or public sector deployment of AI systems: Countries must consider the adoption of a higher

---

[18] Ibid

[19] Niti Aayog, *Working Document: Towards Responsible AI for All* (2020), *available at* <https://niti.gov.in/sites/default/files/2020-07/Responsible-AI.pdf>

[20] Article 14, Constitution of India,1950

[21] Recognised under Article 21 and Part III of the Constitution of India

[22] Article 19(1)(a), Constitution of India, 1950

[23] Jhalak M. Kakkar and Nidhi Singh, "Building an AI governance framework for India", *available at* <https://ccgnludelhi.wordpress.com/2020/09/18/building-an-ai-governance-framework-for-india/>

regulatory threshold for the use of AI by government institutions, given their potential for impacting citizen's rights. Government use of AI systems that have the potential to severely impact citizens' fundamental rights includes the use of AI in the disbursal of government benefits, surveillance and law enforcement.[24]

ii. Need for overarching principles-based AI regulatory framework: Different sectoral regulators are currently evolving regulations to address the specific challenges (privacy and others) posed by AI in their sector.[25] While it is vital to harness the domain expertise of a sectoral regulator and encourage the development of sector-specific AI regulations, such piecemeal development of AI principles can lead to fragmentation in the overall approach to regulating AI. Therefore, to ensure uniformity in the approach to regulating AI systems across sectors, it is crucial to put in place a national level horizontal overarching principles-based framework.

iii. Adaptation of sectoral regulation to effectively regulate AI: In addition to an overarching regulatory framework that forms the basis for the regulation of AI, it is equally important to envisage how this framework would work with horizontal or sector-specific laws such as consumer protection law, and the applicability of product liability to various AI systems, and personal data protection frameworks.[26] Traditionally consumer protection and product liability regulatory frameworks have been structured around fault-based claims. However, given the challenges concerning explainability and transparency of decision making by AI systems, it may be difficult to establish the presence of defects in products and, for an individual who has suffered harm, to provide the necessary evidence in court. Hence, consumer protection laws may have to be adapted to stay relevant in the context of AI systems. Even sectoral legislation

---

[24] Akriti Bopanna, 'India's tryst with predictive policing', (*VIDHI Centre for Legal Policy*, April 2020), *available at* <https://vidhilegalpolicy.in/blog/indias-tryst-with-predictive-policing>

[25] See Reserve Bank of India, 'Report of the Working Group on FinTech and Digital Banking' (November 2017) *available at* <https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WGFR68AA1890D7334D8F8F72CC2399A27F4A .PDF>

[26] See European Commission, *Register of Commission Expert Groups, available at* <https://ec.europa.eu/transparency/expert-groups-register/screen/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608>

regulating the use of motor vehicles[27] would have to be modified to enable and regulate the use of autonomous vehicles and other AI transport systems.

iv. Contextualising AI systems for both their safe development and use: To ensure the effective and safe use of AI systems, they have to be designed, adapted and trained on relevant datasets depending on the context in which they will be deployed. The Working Document envisages India being the AI Garage for the world.[28] Additionally, India will likely import AI systems developed in countries such as the US, EU and China to be deployed within the Indian context. Both scenarios involve the use of AI systems in a context distinct from the one in which they have been developed. Without effectively contextualising socio-technical systems like AI systems to the environment they are to be deployed in, there are enhanced safety, privacy, accuracy and reliability concerns.

Currently in India, the Personal Data Protection Bill, 2019 (PDP Bill),[29] is being considered by the Indian Parliament, which contains provisions that will likely apply to the use and processing of personal data by AI systems. The data protection principles relating to notice and consent, purpose limitation, data minimisation, accuracy, storage limitation, security and accountability will likely apply to the use of personal data by AI systems.

As data processing capabilities continue to evolve at a feverish pace, basic data protection principles as envisaged in data protection legislation like the PDP Bill 2019 might not be sufficient to address new challenges. For example, big data analytics may render traditional notions of consent meaningless as users have limited to no knowledge of how such algorithms behave, how the data is being used, the purpose for which it is being processed and what determinations are made by such technology.[30] Additionally, given that AI systems rely significantly on anonymised personal data, their use of data may not fall squarely within the regulatory domain of

---

[27] The Motor Vehicles Act, 1988 (India)

[28] Niti Aayog, *Working Document: Towards Responsible AI for All* (2020), *available at* <https://niti.gov.in/sites/default/files/2020-07/Responsible-AI.pdf>

[29] The Personal Data Protection Bill, 2019 (introduced in Lok Sabha on December 11, 2019) < http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf>

[30] Martin Tisné & Marietje Schaake, 'The Data Delusion: Protecting Individual Data Isn't Enough When the Harm is Collective, (2020) Cyber Policy Centre', *available at* <https://cyber.fsi.stanford.edu/publication/data-delusion>

the PDP Bill. The PDP Bill does not apply to the regulation of anonymised data at large but the Data Protection Authority has the power to specify a code of practice for methods of de-identification and anonymisation, which will likely impact AI technologies' use of data. [31]

The Bill also contains some provisions which seek to impose data localisation requirements.[32] There is a growing trend of the Indian government and regulators imposing localisation requirements on certain categories of data for a variety of stated reasons including to increase privacy and security.[33] For example, the Reserve Bank of India issued a notification directing that payment system providers must 'ensure that the entire data relating to payment systems operated by them are stored in a system only in India'.[34] Similarly, a draft of the e-commerce policy stated that steps would be taken to develop capacity for and incentivise domestic data storage in India and post a two year sunset period, data localisation would become mandatory.[35] The policy states that data stored in India will be shared with local start-ups meeting certain criteria. It is not clear how consent, purpose limitation or any other requirements under the PDP Bill will play into this.[36]

Another key policy development in the Indian context is the Report by the Committee of Experts on Non-Personal Data Governance Framework ('NPD Report').[37] The Report proposes to create a regime for mandatory non-personal data (anonymised and deidentified personal data) sharing between businesses, communities and the government in order to unlock the "social/public/economic" value of data".[38] The Report notes that 'abundant availability of data is a primary driver for AI' (and therefore,

---

[31] Clause 2 and Clause 50, PDP Bill, *supra* note 29
[32] Clause 33, PDP Bill, *supra* note 29
[33] See Comments On The Draft Personal Data Protection Bill 2018 (PDP Comments CCG), Centre For Communication Governance At National Law University Delhi (2018), *available at* <https://ccgdelhi.org/wp-content/uploads/2018/10/CCG-NLU-Comments-on-the-PDP-Bill-2018-along-with-Comments-to-the-Srikrishna-Whitepaper.pdf>
[34] Storage of Payment System Data, RBI/2017-18/153 (2018).
[35] Aroon Deep, 'Draft National E-Commerce Policy: Data Localisation and Priority to Domestic Companies', (*Medianama,* August 7, 2018), *available at* <https://www.medianama.com/2018/08/223-draft-national-e-commerce-policy-datalocalisation-and-priority-to-domestic-companies/>
[36] PDP Comments, *supra* note 33
[37] Ministry of Electronics and Information Technology, *Report by the Committee of Exports on Non-Personal Data Governance Framework* (2020)*, available at* <https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/08/mygov_159453381955063671.pdf>
[38] Ibid, Key Take-aways- Case for regulating data p 11.

access to non-personal data will help increase its revenue from analytics and machine learning services) and seeks to enable the domain of AI in India.[39] The report suggests the use of models of data fiduciaries and data trusts and introduces concepts such as community data and community privacy.[40] The Committee Report has appreciable suggestions while also having concerning proposals and we have engaged with these proposals and provided input in a response to the Committee.[41]

One of the key proposals of the Committee is the setting up of data trusts, though in the Committee Report several questions around their structure and role remain unaddressed.[42] In literature, data trusts are considered 'intermediaries that aggregate user interests and represent them more effectively vis-à-vis data processors.'[43] In the age of Big Data, it is useful for countries around the world to explore alternate models of data governance such as data trusts, data cooperatives, and data commons to safeguard the privacy of individuals and empower their decision making in the context of the use of their data.

To solve issues of information asymmetries and power imbalances between users and data processors, institutions such as data trusts act as facilitators of data flow between the two parties, but on the terms of the users.[44] Data trusts typically act with a fiduciary duty and have the mandate to act in the best interests of their members.[45] They have the requisite legal and technical knowledge to act on behalf of users. Instead of users making potentially ill-informed decisions over data processing, data trusts make these decisions on their behalf, based on pre-decided factors like a bar on third-party

---

[39] Ibid para 3.2. ii.

[40] Centre for Communication Governance, 'Comments on the Report by the Committee of Experts on Non-Personal Data Governance Framework, 2020', *available at* <https://ccgdelhi.org/wp-content/uploads/2020/09/CCG-NLU-Comments-to-MeitY-on-the-Report-by-the-Committee-of-Experts-on-Non-Personal-Data-Governance-Framework.pdf>

[41] Ibid

[42] Report by the Committee of Exports on Non-Personal Data Governance Framework, *supra* note 37.

[43] Aline Blankertz, 'Designing Data Trusts: Why We Need to Test Consumer Data Trusts Now' (February 2020) *available at* <https://www.stiftung-nv.de/sites/default/files/designing_data_trusts_e.pdf>; Data for Empowerment', (*The Mozilla Foundation*), *available at* <https://foundation.mozilla.org/en/data-futures-lab/data-for-empowerment/readme-about-this-research/>

[44] Sylvie Delacroix & Neil D Lawrence, 'Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance' (2019)9(4) International Data Privacy Law 236, *available at* < https://doi.org/10.1093/idpl/ipz014>

[45] Aditi Agrawal, 'What Are Data Trusts? How Do They Work?' (Medianama) *available at* < https://www.medianama.com/2020/08/223-nama-data-trusts/>

sharing.[46] For example, data trusts to users can be what mutual fund managers are to potential investors in capital markets.[47]

Currently, in a typical transaction in the data economy, if users wish to use a particular digital service or provide consent for the use and processing of their data, they typically do not have the knowledge to understand the possible privacy risks nor the bargaining power to address their concerns. Data trusts with a fiduciary responsibility towards users, specialised knowledge, and better bargaining power given that they represent multiple members, are better placed to tilt the power dynamics in favour of users. Data trusts might be relevant from the perspective of both the protection and controlled sharing of personal as well as non-personal data, more broadly for the digital economy as well as for the AI industry more specifically.

Though solutions like data trusts seem promising, they would have to be thoroughly tested and experimented with before wide-scale implementation.[48] In the Indian context, existing law may have to be reworked since this would be a new form of trust, and data as a subject matter of the trust is not envisaged by Indian law.[49] Additionally, though the NPD Report seems to propose data trusts as data sharing institutions, there are concerns about the extent to which they will function as data managers or data stewards, as being suggested above and several questions around their structure and functioning will need to be detailed.[50]

Policymakers in India are at a crucial juncture around framing a personal data protection legislation and experimenting with different models of data governance. It is imperative that these frameworks and models be firmly centred around the protection and preservation of the privacy and data protection rights of Indians, both from private and public entities.[51]

---

[46] Sylvie Delacroix and Neil D. Lawrence, *supra* note 44

[47] Shashank Mohan, 'Experimenting with New Models of Data Governance – Data Trusts' <https://ccgnludelhi.wordpress.com/2020/10/16/experimenting-with-new-models-of-data-governance-data-trusts/>

[48] Comments on the Report by the Committee of Experts on Non-Personal Data Governance Framework, 2020, *supra* note 40.

[49] See The Indian Trusts Act, 1882, s 8

[50] Comments on the Report by the Committee of Experts on Non-Personal Data Governance Framework, 2020, *supra* note 40.

[51] Ibid