



CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY DELHI

INPUTS TO THE GLOBAL DIGITAL COMPACT

APRIL 2023

nludelhi.ac.in | ccgdelhi.org | ccg@nludelhi.ac.in



Centre for Communication Governance
National Law University Delhi
Sector 14, Dwarka,
New Delhi – 110078

Patrons: Professor (Dr.) G.S. Bajpai (Vice Chancellor, NLUD), Professor (Dr.) Harpreet Kaur (Registrar, NLUD)

Faculty Advisor, CCG: Dr. Daniel Mathew

Executive Director, CCG: Jhalak M. Kakkar

Authors: Swati Punia, Joanne D'Cunha, Tejaswita Kharel, and Ananya Moncourt;
Reviewed and edited by Jhalak M Kakkar and Swati Punia

This policy input was made possible by the generous support we received from the National Law University Delhi (NLUD). The Centre for Communication Governance (CCG) would therefore like to thank our patrons, the Vice Chancellor Professor (Dr.) G.S. Bajpai and the Registrar Prof. (Dr.) Harpreet Kaur of NLUD for their guidance. CCG would also like to thank our Faculty Advisor Dr. Daniel Mathew for his continuous direction and mentorship.

Suggested citation – Centre for Communication Governance, 'Inputs to the Global Digital Compact' (2023)



(CC BY-NC-SA 4.0)

ABOUT THE NATIONAL LAW UNIVERSITY DELHI

The National Law University Delhi is one of the leading law universities in the capital city of India. Established in 2008 (by Act. No. 1 of 2009), the University is ranked second in the National Institutional Ranking Framework for the last five years. Dynamic in vision and robust in commitment, the University has shown terrific promise to become a world-class institution in a very short span of time. It follows a mandate to transform and redefine the process of legal education. The primary mission of the University is to create lawyers who will be professionally competent, technically sound and socially relevant, and will not only enter the Bar and the Bench but also be equipped to address the imperatives of the new millennium and uphold the constitutional values. The University aims to evolve and impart comprehensive and interdisciplinary legal education which will promote legal and ethical values, while fostering the rule of law.

The University offers a five year integrated B.A., LL.B (Hons.) and one-year postgraduate masters in law (LL.M), along with professional programs, diploma and certificate courses for both lawyers and non-lawyers. The University has made tremendous contributions to public discourse on law through pedagogy and research. Over the last decade, the University has established many specialised research centres and this includes the Centre for Communication Governance (CCG), Centre for Innovation, Intellectual Property and Competition, Centre for Corporate Law and Governance, Centre for Criminology and Victimology, and Project 39A. The University has made submissions, recommendations, and worked in advisory/consultant capacities with government entities, universities in India and abroad, think tanks, private sector organisations, and international organisations. The University works in collaboration with other international universities on various projects and has established MoU's with several other academic institutions.

ABOUT THE CENTRE FOR COMMUNICATION GOVERNANCE

The Centre for Communication Governance at the National Law University Delhi (CCG) was established in 2013 to ensure that Indian legal education establishments engage more meaningfully with information technology law and policy and contribute to improved governance and policy making. CCG is the only academic research centre dedicated to undertaking rigorous academic research in India on information technology law and policy in India and in a short span of time has become a leading institution in Asia. Through its academic and policy research, CCG engages meaningfully with policy making in India by participating in public consultations, contributing to parliamentary committees and other consultation groups, and holding seminars, courses and workshops for capacity building of different stakeholders in the technology law and policy domain.

CCG has built an extensive network and works with a range of international academic institutions and policy organisations. These include the United Nations Development Programme, Law Commission of India, NITI Aayog, various Indian government ministries and regulators, International Telecommunications Union, UNGA WSIS, Paris Call, Berkman Klein Center for Internet and Society at Harvard University, the Center for Internet and Society at Stanford University, Columbia University's Global Freedom of Expression and Information Jurisprudence Project, the Hans Bredow Institute at the University of Hamburg, the Programme in Comparative Media Law and Policy at the University of Oxford, the Annenberg School for Communication at the University of Pennsylvania, the Singapore Management University's Centre for AI and Data Governance, and the Tech Policy Design Centre at the Australian National University.

The Centre has had multiple publications over the years including the Hate Speech Report, a book on Privacy and the Indian Supreme Court, and most recently an essay series on Democracy in the Shadow of Big and Emerging Tech. The Centre has launched freely accessible online databases - Privacy Law Library (PLL) and High Court Tracker (HCT) to track privacy jurisprudence across the country and the globe in order to help researchers and other interested stakeholders learn more about privacy regulation and case law. CCG also has an online 'Teaching and Learning

Resource' database for sharing research-oriented reading references on information technology law and policy. In recent times, the Centre has also offered courses on AI Law and Policy, Technology and Policy, and first principles of cybersecurity. These databases and courses are designed to help students, professionals, and academicians build capacity and ensure their nuanced engagement with the dynamic space of existing and emerging technology and cyberspace, their implications for the society, and their regulation. Additionally, CCG organises an annual International Summer School in collaboration with the Hans Bredow Institute and the Faculty of Law at the University of Hamburg in collaboration with the UNESCO Chair on Freedom of Communication at the University of Hamburg, Institute for Technology and Society of Rio de Janeiro (ITS Rio) and the Global Network of Internet and Society Research on contemporary issues of information law and policy.

TABLE OF CONTENTS

1. COMMITMENTS FOR A SECURE AND INCLUSIVE DIGITAL ECOSYSTEM...	1
2. OVERVIEW OF KEY PRINCIPLES.....	2
3. INTRODUCTION.....	4
4. PRINCIPLE 1: PRIVACY.....	6
5. PRINCIPLE 2: SECURITY.....	14
6. PRINCIPLE 3: MEANINGFUL TRANSPARENCY.....	20
7. PRINCIPLE 4: ACCESS TO ALL.....	29
8. PRINCIPLE 5: INFORMATIONAL SELF DETERMINATION.....	37
9. CONCLUSION.....	43

COMMITMENTS FOR A SECURE AND INCLUSIVE DIGITAL ECOSYSTEM

Reconcile new and existing rights and principles with emerging digital rights to create a secure digital world

Foster global alignment and understanding on norms, principles, and standards that promote shared values and interests as well as create a baseline of common lexicon, rights and technical standards

Leverage technology to bridge the digital divide and empower those who have been historically marginalised

Ensure convergence in laws and regulations across jurisdictions along with harmonisation of technical standards

Establish the right to privacy as a fundamental right to secure dignity and autonomy of individuals in the digital world to actualise other economic, social, cultural rights

Embed security in the different layers of the digital ecosystem through security-by-design and privacy-by-design in digital technologies

Ensure transparency measures are curated in a manner that keeps local context, the type of the recipient and the end-value in mind

Integrate and implement access to social justice within access to technology to build a just and fair digital world

Allow space for honest and free expression of oneself for individual development and to sustain a vivid democratic society

Overview of Key Principles



Data Protection |



Artificial Intelligence |



Platform Accountability

Principle 1 : Privacy



- Make data protection principles the core of legislation
- Provide safeguards to exemptions



- Create agile and iterative privacy protection frameworks in AI
- Mandate periodic audits for compliance with privacy regulations



- Create human rights and privacy focused platform regulation

Principle 2: Security



- Incorporate technical and physical security measures
- Efficient security standards evolve with technology
- Adopt risk-based approach to data protection
- Encourage regulatory sandboxes for assessment and development of security standards and safeguards



- Establish safety assessment frameworks in AI systems

Principle 3: Meaningful Transparency



- Mandate transparency and accountability requirements
- Demonstrate compliance through fair and lawful processing
- Encourage ex-ante transparency standards



- Incorporate transparency in design and implementation of AI systems
- Mandate human oversight in AI systems



- Contextualise transparency measures based on audience and purpose
- Develop unified best practices with detailed guidelines to create a uniform baseline of transparency

Principle 4: Access for All



- Incorporate the right to access information and to object to automated processing
- Balance freedom of speech and expression and the right to correction and erasure
- Create accessible grievance redressal systems
- Adopt graded approach to parental control
- Consider best interest of children



- Establish mechanisms for greater user control over decisions made on platforms

Principle 5: Informational Self Determination



- Empower users through added obligations on data processors and controllers to act in best interest of users
- Create a baseline level of protection and rights across borders
- Recognise the right to be forgotten



- Build inclusivity in different levels of AI system to minimise the risk of bias



- Increase user awareness of platform harms, user control on platforms and accessing grievance redressal mechanisms

INTRODUCTION

The constant evolution and development of technology has provided great societal benefit but has equally led to the emergence of new forms of inequalities and discrimination in the digital world. To identify and address the risks and harms emanating from the digital transformation of the world, it is crucial to understand their source and the functioning of technologies that contribute to such harms and risks. This is especially important for emerging and developing economies of the Global Majority that often lack adequate regulatory mechanisms to protect internet users and citizens in the digital world.

An important aspect of creating an inclusive digital world lies in both recognising new rights and reconciling existing rights and principles with emerging digital rights. In order to achieve this vision, it is crucial to foster global alignment on norms, principles, and standards that promote our shared values and interests. Such frameworks need to balance rights and interests of individuals and communities to accommodate diverse global contexts and realities. Fundamental human rights such as the right to privacy and the right to equality are interlinked with civil and political rights such as the right against discrimination, right to freedom of opinion and expression, right to freedom of peaceful assembly and association, etc. They ought to be embedded in the digital space for realising other economic, social and cultural rights and for the sustainable development of democratic societies.

It is necessary to assess the development of technology in a manner that enables the creation of opportunities and access for all sections of the society. Needs of diverse linguistic, cultural and geographical communities should be accounted for to alleviate inequality. In particular, technology should be leveraged to bridge the gap for those who have been historically marginalised and continue to be on the fringes of the digital realm. Assessing the types of human rights standards such as ethics, privacy, freedom of expression, etc. and the manner of their implementation in different domains of technology like artificial intelligence and platform governance will help achieve a rights protecting and socially secure digital ecosystem. In addition, it is also pertinent to identify gaps in current global human rights frameworks that do not sufficiently account for existing and future risks that might occur due to the rapid development of technology in the digital world.

To operationalise such a baseline level of protections, there needs to be convergence in laws and regulations across jurisdictions along with harmonisation of technical standards that have wide implications on human rights, sustainable development of economies, and geopolitics. Building a common understanding on all these levels is a prerequisite for designing effective frameworks and measures to contain negative implications of technology. An often overlooked dimension in realising this vision is

the fractured understanding of key concepts and terminologies adding to unnecessary confusion and compromising much needed clarity for realising the goals of the UN Common Agenda. For instance, the lack of uniformity in understanding the terminologies and tools and techniques within the taxonomy of de-identification. In the context of data protection frameworks, the terms anonymisation and pseudonymisation hold varied interpretations for different stakeholder groups and jurisdictions across the globe.¹ A common lexicon is necessary to weed out unintended structural discrepancies that act as an impediment to build harmony and trust between different actors of the digital world.

This submission aims to outline five key principles to facilitate an open, free and secure digital future for all, in the context of the United Nations efforts to convene a Global Digital Compact. These principles include privacy, security, meaningful transparency, access, and informational self determination. These shared principles can help ground global digital co-operation efforts in common objectives. This submission will examine the applicability of each of the five key principles in the specific context of three key domains of our global digital ecosystem: (a) Data Protection (b) Artificial Intelligence (AI) and (c) Platform Accountability. A point to note here is that there needs to be greater focus on overall platform governance within the themes identified in the Global Digital Compact. Platforms are known to play a crucial role in larger democratic processes, and they significantly impact the rights of users - of privacy, speech and expression, and anti-discrimination. Therefore, there is value in looking beyond the accountability of platforms for specific types of content and how platforms can be held accountable for harms resulting from their operation and use. The fundamental principles discussed below highlight key concerns and provide specific recommendations to help realise the goals of the Global Digital Compact and the UN Common Agenda.

¹ Centre for Communication Governance, *Drafting Data Protection Legislation: A Study of Regional Frameworks* (UNDP 2023) 21 <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/undp-drafting-data-protection-legislation-march-2023-443.pdf>>.

PRIVACY

Principle 1

Key Recommendations for Privacy

Privacy as a concept and as a key principle should be incorporated in the design, development, and use of technology as well as standards and regulations shaping the interaction of technology and users in the digital world. Recognising the right to privacy as a fundamental right is essential for securing dignity and autonomy of individuals in the digital world as it plays an intrinsic role in the actualisation of other economic, social and cultural rights.

DATA PROTECTION



An efficient data protection framework should incorporate data protection principles as the minimum set of guidelines to operationalise informational privacy and to assign individual agency over their data.

Exemptions to data protection laws and provisions must be subject to internationally accepted safeguards such as necessity and proportionality, legitimate aim and should adhere to technical security standards.



ARTIFICIAL INTELLIGENCE

Agile and iterative privacy protection frameworks are necessary for AI systems which are constantly evolving and extremely opaque to ensure that privacy and ethical considerations are incorporated at every stage of the design and development of AI systems to avoid infringement of individuals' rights. Measures such as privacy by design, ethics by design, and periodic audits are some of the ways in which this can be implemented.

Periodic audits of AI systems should be mandated to ensure compliance with privacy regulations and data protection principles like transparency, purpose limitations, and to identify any new or potential risks.

PLATFORM ACCOUNTABILITY



Algorithmic systems and incentives driving platforms cause concerns of discriminatory and misleading content, misinformation, curtailment of freedom of speech and expression which often involve great risks to user privacy. A human rights focused approach should be adopted for regulating platforms and algorithmic processes. The Santa Carla principle for content moderation is a good example for securing privacy and data protection.

INTRODUCTION

The right to privacy has been recognised in international law and is key to exercising basic human rights both online and offline. Article 12 of the Universal Declaration of Human Rights² states that ‘No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation’. Article 17 of the International Covenant on Civil and Political Rights³ also states that ‘Everyone has the right to the protection of the law against such interference or attacks’.

In 2017, the Supreme Court of India in *Puttaswamy vs. Union of India*⁴ recognised that the right to privacy is a fundamental right and currently, the edifice of the constitutional right to privacy is evolving and expanding through subsequent cases in state level courts as well. The right has been built on the foundations of autonomy, dignity and liberty - values that are deeply entrenched in the Indian Constitution. Privacy as a concept and as a key principle should be incorporated in the design, development, and use of technology as well as standards and regulations shaping the interaction of technology and users in the digital world.



PRIVACY AS THE FOUNDATION OF DATA PROTECTION FRAMEWORKS

The collection and use of data by companies, governments and other data collectors and processors needs to be regulated to prevent misuse and necessitate security safeguards and barriers. To achieve adequate protection of users and their data, data protection frameworks need to be anchored by the right to privacy.⁵

² Universal Declaration of Human Rights (Adopted 10 December 1984) UNGA Res 217 A(III) (UDHR), art 5 <https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/eng.pdf>.

³ International Covenant on Civil and Political Rights (Adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR), art 17 <<https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>>.

⁴ *Justice K.S. Puttaswamy (Retd.) and Anr. v Union of India and Ors.* (2017) AIR 2017 SC 4161 <<https://privacylibrary.ccgndud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors>>.

⁵ Centre for Communication Governance, *Comments to the Ministry of Electronics and Information Technology on the Draft Digital Personal Data Protection Bill, 2022* (CCG 2022) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-to-meity-on-the-draft-digital-personal-data-protection-bill-2022-334.pdf>>.

RECOMMENDATIONS

Privacy intrinsic to actualisation of other key rights

The right to privacy is essential for securing dignity and autonomy of individuals in democratic societies of the digital era.⁶ It is an intrinsic part of other constitutional rights such as the right to life and personal liberty and the right to equality and helps in the realisation of civil political rights and freedoms: of speech and expression, of movement, and of association, among others. With technology underpinning our private and public lives, data is being collected and shared at an unprecedented scale to create new services and goods for the digital economy, governance, and users. Unfortunately, this phenomenon coincides with innumerable data breaches and leaks placing privacy and other rights at risk, especially in jurisdictions lacking measures to protect the privacy, information and data of its people. Hence, operationalising a comprehensive data protection legislation is essential for protecting the informational privacy and basic human rights including the right to privacy in the digital world.

A robust data protection framework is built on data protection principles

Data protection principles are considered the minimum set of guidelines an effective data protection framework should incorporate to operationalise informational privacy and to assign individual agency over data.⁷ These principles govern the data lifecycle from collection to processing to sharing of data and sets out clear roles and responsibilities of those engaged in these activities. Individual participation, purpose limitation, data minimisation, limits on data retention and collection, privacy-by-design, adequate and appropriate technical safeguards and security measures like encryption of data are some of the key privacy preserving measures which ought to feature in an effective data protection regime.⁸ The operationalisation of these core privacy preserving principles need to be done not only through regulations and creation of legal obligations but also by incentivising market actors to build and adopt privacy-enhancing measures in building technology.

⁶ Justice K.S. Puttaswamy (Retd.) and Anr. v Union of India and Ors. (2017) AIR 2017 SC 4161 <<https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors>>.

⁷ Centre for Communication Governance, *Drafting Data Protection Legislation: A Study of Regional Frameworks* (UNDP 2023) 36-51 <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/undp-drafting-data-protection-legislation-march-2023-443.pdf>>; Centre for Communication Governance, *Comments to the Ministry of Electronics and Information Technology on the Draft Digital Personal Data Protection Bill, 2022* (CCG 2022) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-to-meity-on-the-draft-digital-personal-data-protection-bill-2022-334.pdf>>.

⁸ *ibid.*

Safeguards to exemptions

States may often grant exemptions to themselves or other non-governmental bodies from complying with certain aspects of the data protection regime. This is usually done for purposes such as investigation and detection of crimes, national security, journalistic and literary purposes, research, historical or statistical purposes. While such exemptions are necessary, there is potential for their abuse and misuse. In order to balance the rights of the users and citizens and the need for state exemptions in certain circumstances, it is pertinent that any such exemption be subject to internationally accepted safeguards such as necessity and proportionality,⁹ legitimate aim,¹⁰ etc. Further, there should be no exemption from maintaining technical security standards, protecting children from harm and ensuring accuracy of data. Principles such as storage limitation, and data minimisation, etc. which do not unduly restrict the actions of the bodies undertaking such works should not be exempted.¹¹



PRIVACY-PROTECTING ARTIFICIAL INTELLIGENCE

AI systems should be designed and operationalised in a manner that respects and protects the privacy of individuals and their personal data. Privacy concerns arise at all stages of the AI system's development and deployment including data collection, storage, and usage.¹² It is essential to ensure that privacy is a key determinant while conceptualising AI systems to prevent any potential misuse or the ability of AI to track, identify, exclude or cause harm to individuals.

There are certain data protection principles such as purpose specification, use limitation, and data minimisation that apply to the use and processing of data in AI

⁹ Centre for Communication Governance, *Comments to White Paper of the Committee of Experts on a Data Protection Framework for India* (CCG 2018) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-on-the-pdp-bill-2018-along-with-comments-to-the-srikrishna-whitepaper-396.pdf>>; *EU General Data Protection Regulation (GDPR)*: Regulation (EU) 2016/679 (27 April 2016), art 23.

¹⁰ UN Human Rights Council, *The Right To Privacy In The Digital Age: Report Of The Office Of The United Nations High Commissioner For Human Rights*, UN Doc A/HRC/27/37 (2014) <https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf>.

¹¹ Centre for Communication Governance, *Comments to the Ministry of Electronics and Information Technology on the Draft Digital Personal Data Protection Bill, 2022* (CCG 2022) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-to-meity-on-the-draft-digital-personal-data-protection-bill-2022-334.pdf>>.

¹² Centre for Communication Governance, *Response To Call For Inputs For The Report On 'the Right To Privacy In The Digital Age'* (CCG 2021) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-comments-on-the-thematic-report-on-the-right-to-privacy-in-the-digital-age--250.pdf>>.

systems. Often, AI models require large volumes and variations of data to be trained, and the functioning of advanced AI systems can pose challenges to the application of data protection principles. The tension between AI systems and certain data protection principles arises due to the unpredictable or unforeseen results that can be produced by advanced AI models. There also exist some unique features of AI systems, such as the “black box effect”, that can impact user privacy. In certain cases, it is not yet possible for the treatment of data by AI systems to be articulated or identified by humans as a logical flow of decisions. This may pose unique challenges around the effective protection of data and privacy of individuals.

RECOMMENDATIONS

Agile and iterative privacy protection frameworks

The “black box” associated with the use of AI¹³ and the lack of complete knowledge about how the algorithm works means that exercising control over the data and how AI systems use it at various stages becomes increasingly difficult. Implementation of a privacy-by-design¹⁴ and ethics-by-design¹⁵ approach, which incorporates privacy and ethical considerations into every stage of the AI system's development, are critical to avoid infringement of individual's rights. Clear and transparent privacy policies should be developed and communicated to users, detailing the type of data collected, how it will be used, and who will have access to it.

Periodic audits of AI systems

Concerns for the protection of privacy arise from the ability of AI systems to enable data exploitation¹⁶ and re-identification of de-identified or anonymised data. For example, datasets are often de-identified to remove or replace specific individual identifying information before they are shared as outputs. However, current technology makes it possible for AI systems to reverse this process to re-identify such

¹³ AJ Abdallat, Explainable AI: Why We Need To Open The Black Box (*Forbes*, 22 Feb 2019) <<https://www.forbes.com/sites/forbestechcouncil/2019/02/22/explainable-ai-why-we-need-to-open-the-black-box/?sh=36dc84441717>>.

¹⁴ Privacy by design is an approach that embeds privacy and security into the design and operation of a product and its network. It seeks to make privacy the ‘default setting’ rather than a post-facto consideration, Ann Cavoukian, “Privacy by Design - The 7 Foundational Principles” (IAPP).

¹⁵ European Commission, *Ethics by Design and Ethics of Use Approaches for Artificial Intelligence* (25 November 2021) <https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf>.

¹⁶ Privacy International, ‘Artificial Intelligence’ <<https://privacyinternational.org/learn/artificial-intelligence>>.

personal data.¹⁷ The deployment of AI solutions in sectors like finance and healthcare for instance, require heightened privacy safeguards due to the sensitive and confidential nature of personal information that is dealt with. To further enhance privacy, AI systems should be audited at regular periodic intervals to ensure compliance with privacy regulations, to identify any new or potential risks or impact and to assess compliance with purpose limitation requirements. It is also important for guidelines, regulations and compliance mechanisms to evolve with advances in technology to ensure that protection of privacy is sustained over time.¹⁸ For instance, owing to developments in technology and de-anonymisation AI tools, anonymisation as a technique to protect privacy is also fallible. Therefore, as the diversity of AI applications and their combination with other technology systems increases, privacy protecting mechanisms may need to evolve and considerations for privacy need to be accounted for at legal and technical levels.



HUMAN-RIGHTS FOCUSED ALGORITHMIC SYSTEMS

Algorithmic systems used by social media platforms, such as recommender systems, are known to operate in a manner that contributes to a range of harms such as discriminatory and misleading content, misinformation, privacy concerns, and those that impact freedom of speech and expression. In order to address these harms more broadly, mandating human rights to feature at all stages of algorithmic processes is crucial. Algorithms on platforms, by way of their design, utilise large amounts of user data to tailor content and advertisements based on user preferences. However, platforms also exploit user data by collecting information on behaviours and interactions with the platform, to increase user-engagement¹⁹ for purposes that have not been explicitly consented to by users. Users are shown hyper-targeted advertising²⁰ and viral content which allows data of such users to be collected when

¹⁷ Luc Rocher, J.M. Hendrickx & Y. de Montjoye, 'Estimating the success of re-identifications in incomplete datasets using generative models' (*Nature Comm*, 2019) <<https://www.nature.com/articles/s41467-019-10933-3>>.

¹⁸ Centre for Communication Governance, *Response To Call For Inputs For The Report On 'the Right To Privacy In The Digital Age'* (CCG 2021) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-comments-on-the-thematic-report-on-the-right-to-privacy-in-the-digital-age--250.pdf>>.

¹⁹ Nathalie Maréchal and Ellery Roberts Biddle, 'It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge' (*New America*, 17 March 2020) <<http://newamerica.org/oti/reports/its-not-just-content-its-business-model/>>.

²⁰ Dr. Nathalie Maréchal, 'Targeted Advertising Is Ruining the Internet and Breaking the World' (*Vice*, 17 November 2018) <<https://www.vice.com/en/article/xwjden/targeted-advertising-is-ruining-the-internet-and-breaking-the-world>>.

they engage with such content.²¹ When there are no restrictions on what data is collected or what it is used for in these circumstances, the privacy of individuals are put at risk.²² Therefore, an important aspect of establishing human-rights focused systems is considering the role algorithms play in allowing for privacy harms.

RECOMMENDATIONS

Ensure privacy of users on platforms

The Santa Clara Principles for content moderation is a good example of how to incorporate a human-rights focused approach to platform governance.²³ Algorithms such as recommender systems used by platforms can be designed and operated in a manner that does not infringe upon user privacy - for instance, by collecting only necessary information. Regulation through data protection frameworks can help mandate limited collection of user data. Additionally, ensuring that human rights is a core consideration can be demonstrated in many forms, such as requiring that rules and policies of platforms disclose the manner in which user privacy is kept at the centre of its processes. Ensuring that platforms conduct human rights impact assessments to identify and solve for how its systems impact user rights and fundamental freedoms is another good example of the role that regulation can play.

²¹ Nathalie Maréchal and Ellery Roberts Biddle, 'It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge' (New America 17 March 2020) <<http://newamerica.org/oti/reports/its-not-just-content-its-business-model/>>.

²² *ibid.*

²³ Santa Clara Principles on Transparency and Accountability in Content Moderation <<https://santaclaraprinciples.org/>>.

SECURITY

Principle 2

Key Recommendations for Security

Embedding security in different layers of the digital ecosystem is crucial in implementing the principle of privacy. Besides mandating security standards through regulations, States need to design policies that incentivises the market to adopt security and privacy first approach to create a push for technology that adopts security-by-design and privacy-by-design.

DATA PROTECTION

Any kind of data processing must comply with different types of data security obligations such as organisational, administrative, technical and physical security measures to protect personal data.

Standards for what constitutes appropriate and reasonable measures should evolve with the pace of technology and existing best practices.

Data protection frameworks must establish a risk-based approach to ensure that processing of data with higher risk would require higher security standards and safeguards. While de-identification measures should be incentivised, only data that is unreasonably difficult or impossible to re-identify should be considered as anonymous. Restrictions and penalties must be imposed on the identification and re-identification of de-identified data.

To develop efficient standards, regulatory sandboxes may be explored to assess the need for new standards and safeguards and efficiency of existing ones.



ARTIFICIAL INTELLIGENCE

It is imperative to establish assessment frameworks that necessitate safety and reliability measures throughout the lifecycle of AI systems in order to build continuous risk management systems to address concerns in AI systems. Ensuring human intervention is an important component of ensuring safety and reliability of an AI system.

INTRODUCTION

Across time zones, data breaches and leak incidents are on a rise leading to significant cost to the economy and lead to irreparable harm to sections of the society. Embedding security in different layers of the digital ecosystem is crucial in implementing the principle of privacy. Adequate safeguards and security standards for processing data need to be established through technical and organisational measures and legal provisions that help prevent privacy violations. States need to design policies that incentivises the market to adopt security and privacy first approach to create a push for technology that adopts the principles of security-by-design and privacy-by-design.

The regulation of the digital space ought to be done in a manner wherein security standards and privacy are not deemed as mutually exclusive, and instead, security strategies should be based on the principles of privacy and ethics. However, the vulnerabilities of the digital world have presented new challenges for the law enforcement agencies and concerns for national security. This scenario often makes a case for relaxation of security standards like end-to-end encryption for investigation purposes leading to possible violations of privacy and confidentiality of users. In exceptional circumstances like national security or public order where it becomes necessary to prioritise state security over user privacy, the principles of proportionality and necessity must be complied with.



SECURITY AND SAFEGUARDS IN DATA PROTECTION FRAMEWORKS

In order to protect the right to privacy of the users, processing of data should only take place if appropriate organisational, administrative, physical, and technical safeguards and procedures have been implemented in order to protect the security of personal data. It is important to ensure that personal data is protected against or from unauthorised or accidental access, damage, loss or other risks presented by data processing.

RECOMMENDATIONS

Mandating Data Security Obligations

Data Security is recognised as a key principle of data protection and helps prevent accidental or unlawful destruction, loss, alteration, and unauthorised disclosure or access to personal data. The objective of incorporating data security within data protection frameworks is to protect the confidentiality, integrity, and availability of personal data. This ensures that only those authorised to do so can access, alter, delete or disclose data within the limits of their authority. With such security safeguards, the

accuracy and completeness of data is maintained and data is made accessible, usable, and recoverable.²⁴

In order to ensure that data security measures are implemented, data protection frameworks must have provisions creating obligations on data controllers and processors to ensure adequate data security. Appropriate and reasonable technical and organisational measures ought to be incorporated into security systems by data controllers and processors. Since the standards for appropriate and reasonable measures evolve with time and development in technology, the determination of what is reasonable and appropriate should be based on best-practice and other developing factors. These factors may include the proportionality and necessity of measures taken and the evolution of privacy threats.²⁵ The measures undertaken based on these factors must be subject to periodic review, reassessment, audit, updating and improvement.

Incorporation of technical and organisational security measures

Organisational measures such as anonymisation and pseudonymisation of data is recommended to ensure data security. Such de-identification measures should be incentivised as these processes reduce the risk of direct identification of individuals using personal information that may be misused.²⁶ However, de-identification of data does not make the data immune from breach or prevent harms from occurring as concerns with identification or re-identification continue to exist. Hence, it is important that only data that is unreasonably difficult or impossible to re-identify be considered as anonymous. Although, it must be kept within the purview of the definition of personal information and be made subject to fewer obligations to incentivise this practice.²⁷ As de-identified data faces the risk of identification/re-identification, it is important to have restrictions on the identification and re-identification of such data to protect users. There must also be penalties for identification or re-identification of such data.

In addition to organisational measures, technical measures including both physical measures and Information and Communications Technology (ICT) security measures ought to be incorporated in data processing systems. Physical measures would include the quality of doors and locks, CCTV and policies related to disposal of physical

²⁴ Centre for Communication Governance, *Drafting Data Protection Legislation: A Study of Regional Frameworks*, (UNDP 2023) 63 <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/undp-drafting-data-protection-legislation-march-2023-443.pdf>>.

²⁵ *ibid*.

²⁶ Centre for Communication Governance, *Comments to the Ministry of Electronics and Information Technology on the Draft National Governance Framework Policy, 2022* (CCG 2022) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-to-meity-on-the-draft-national-framework-policy-300.pdf>>.

²⁷ Centre for Communication Governance, *Drafting Data Protection Legislation: A Study of Regional Frameworks* (UNDP 2023) 21-24 <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/undp-drafting-data-protection-legislation-march-2023-443.pdf>>.

materials, while ICT security measures would include security of network and information systems, online security, authorisation and authentication policies and device security, among others.²⁸

Risk-based approach for data protection

Different types of data have different levels of risk and hence, require different levels of security and safeguard standards. The creation of a risk-based data protection regime would aid in ensuring that there are adequate safeguards for data with higher risks.²⁹ Data protection frameworks should be created considering the need for separate levels of regulation for different forms of data.³⁰ The classification of data should be based on the potential risk associated with identification of an individual.³¹ This would ensure that the type of data with a higher risk would have a higher standard of obligation for data controllers and processors.

Regulatory sandboxes for testing security of standards and safeguards

The rapid pace of digital technology requires periodic review, reassessment, audit, updating and improvement in the security standards and safeguards incorporated in systems. In order to determine the need and efficiency of new standards and safeguards, regulatory sandboxes may be created. Such frameworks can be used not only for determining the adequacy of security standards and safeguards in a safe environment but also to help bring in innovative methods to develop efficient standards for privacy and transparency in digital technologies and systems.



SAFE AND RELIABLE AI SYSTEMS

This principle includes ensuring that AI systems are technically reliable and actively promote their security, safety, resilience and robustness. AI systems must reliably operate in accordance with their intended purpose throughout their lifecycle without posing unreasonable safety risks. AI systems also need to be able to deal with direct attacks and attempts to access and manipulate the data or algorithms and flag errors that may arise. These elements of security in AI systems relate to the technical and organisational measures that must be taken to ensure that the system itself meets various security standards including requirements of data protection frameworks. The

²⁸ *ibid* at 63.

²⁹ *ibid*.

³⁰ Centre for Communication Governance, *Comments to the Ministry of Electronics and Information Technology on the Draft Digital Personal Data Protection Bill, 2022* (CCG 2022) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-to-meity-on-the-draft-digital-personal-data-protection-bill-2022-334.pdf>>.

³¹ *ibid*.

security of AI systems should also be considered in the broader context of the safe and reliable use of these systems by users.

An important component of ensuring safety and reliability of an AI system is human intervention or oversight mechanisms. In the context of this principle, the terms "safety" and "reliability" are related concepts but it is important to highlight the distinction between them.³² The reliability of an AI system refers to its ability to withstand unexpected external and/or internal adversities. Reliability is, therefore, a measure of consistency, and it establishes confidence in the safety of a system.³³ Safety refers to an AI system's ability to "do what it is supposed to do, without harming users (human physical integrity), resources or the environment."³⁴

RECOMMENDATIONS

Safety assessment frameworks in AI systems

Processes need to be put in place to assess the safety and reliability of AI systems not only at the time of their deployment but during the entire life cycle of their deployment. AI systems should adopt safety measures which are proportionate to the potential risks, should be continuously monitored and tested to ensure compliance with their intended purpose, and should have a continuous risk management system to address any identified problems. The NIST AI Risk Management Framework,³⁵ or other similar safety assessment frameworks, can be adopted on a voluntary basis as a first step towards practical implementation of this principle. Such oversight mechanisms can help manage, measure and navigate risks posed by AI systems and ensure traceability of datasets, decisions and processes within the AI system.

³² Centre for Communication Governance, *Comments to the Department of Telecom on the Discussion Paper on the Framework for an Indian Artificial Intelligence Stack* (October, 2020) 26 <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-to-dot-on-the-discussion-paper-on-indian-ai-stack-327.pdf>>.

³³ D. Leslie, "Understanding Artificial Intelligence Ethics and Safety" (Alan Turing Institute, 2019) 31 <https://www.turing.ac.uk/sites/default/files/2019-06/understanding_artificial_intelligence_ethics_and_safety.pdf>.

³⁴ High Level Expert Group on Artificial Intelligence set up by the European Commission, "Ethics Guidelines for Trustworthy AI" (2019) 25 <<https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>>.

³⁵ The NIST AI Risk Management Framework (AI RMF) is a voluntary use framework developed to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems. "AI Risk Management Framework" (NIST March 30, 2023) <<https://www.nist.gov/itl/ai-risk-management-framework>>.

MEANINGFUL TRANSPARENCY

Principle 3

Key Recommendations for Meaningful Transparency

Transparency helps build some of the most intrinsic values of rights respecting frameworks: trust, accountability, explainability, verification of information across technologies in the digital ecosystem. It bolsters informed consent and access to information, and helps individuals meaningfully exercise their rights such as understanding and opting out of decision making based solely on automated systems.

DATA PROTECTION



Data protection frameworks must mandate transparency and accountability requirements for any kind of data processing. Data controllers and processors must ‘demonstrate’ compliance with fair and lawful processing and data protection principles.

Ex-ante transparency standards should be encouraged in order to achieve meaningful transparency and ensure accountability on part of those undertaking activities related to data processing. It would ensure that users gain access to information in an intelligible format about all kinds of systems: how their data is used, for what purpose, process or logic involved in creating the output.



ARTIFICIAL INTELLIGENCE

Transparency should be tailored to different stages of AI design and implementation of AI systems in order to ensure trustworthy and explainable AI.

Human autonomy and oversight is critical for defining the objectives of an AI system. Regulatory principles could specify the circumstances and degree to which human oversight is required for AI systems.

PLATFORM ACCOUNTABILITY



Transparency measures need to be contextualised to the local and social context especially in more diverse regions. Hence, unified best practices with detailed guidelines (for areas such as transparency reporting, risk assessments and audits) must be developed to create a uniform baseline to address platform harms. These must be tailored to specific audiences and purposes.

INTRODUCTION

Despite growing voices on the need for integrating transparency in the use and design of technology, the pace at which technology and the digital ecosystem are developing makes it challenging to implement and concretise effective transparency. Transparency helps build some of the most intrinsic values of rights respecting frameworks: trust, accountability, explainability, verification of information across technologies in the digital ecosystem, etc. It bolsters informed consent and access to information, and helps individuals meaningfully exercise their rights such as understanding and opting out of decision making based solely on automated systems.

Automated and autonomous decision-making systems or self-learning systems have changed the way of processing data and extracting value. It often leads to services or outputs that are not part of what can be reasonably expected by a user. These technologies are opaque making it difficult to understand how they function and the manner in which they should be regulated to protect users.



BUILDING TRUST THROUGH TRANSPARENCY, ACCOUNTABILITY AND FAIR AND LAWFUL PROCESSING IN DATA PROTECTION FRAMEWORKS

Transparency and accountability are essential for building trust in the ecosystem and are the core principles of data protection that allow for visibility over a data controller or processor's actions. This ensures that the data controllers and processors are fulfilling necessary duties in order to protect the rights of the users. In furtherance of these principles, requirements for fair and lawful processing of data aid in ensuring that the best interests of the users are being considered and that their rights are not being violated.

RECOMMENDATIONS

Mandating Transparency and Accountability Requirements

Data protection frameworks must mandate transparency and accountability requirements for data controllers and processors such as incorporating privacy-by-design and transparency-by-design in data processing systems, conducting data protection impact assessments at various stages of the data processing process, and

conducting data protection audits to ensure that safeguards are being met.³⁶ A crucial aspect of accountability is also ensuring compensation mechanisms for users in case of data breach, mandating the right to explanation and mandating breach notification amongst others.

Building Ex-Ante Transparency standards

While the above-mentioned measures are vital, in order to achieve meaningful transparency, ex-ante transparency standards help ensure measures take into account the broader ecosystem as well. Taking into consideration the type of system, its purpose, the kinds of data it uses or the users of the system, can help determine how information about these functions and processes are presented to a user or the relevant audience. For instance, consider automated decision making systems, individuals ought to be provided with explanations on how such a system makes use of data or the logic involved in making decisions, and the potential risks from processing. Standards guiding the decision-making process for a relevant system need to be designed keeping in mind these aspects to render information holders accountable. This can further provide users with information on how decisions are made with regard to their data and allow them to practise agency over their data.

Demonstrating compliance to help build transparency and accountability

Any data processing activity must be in accordance with the law and undertaken for ethical purposes. Fair and lawful processing places a check against any harmful, misleading, deceptive, and discriminatory processing of data by mandating data controllers and processors to clearly inform the users about how they use users' data and hence, helps build transparency and accountability in the ecosystem.³⁷

The principle of fair and lawful processing is crucial for building the pillars of trust, transparency and accountability in the digital ecosystem. By mandating demonstration of compliance with all other principles of data protection, it helps ensure that data processing activities are being undertaken in the best interest of users. However, for effective implementation of this principle, it is necessary to provide clear guidance to data controllers and processors on their responsibilities and duties when

³⁶ Centre for Communication Governance, *Drafting Data Protection Legislation: A Study of Regional Frameworks* (UNDP 2023) 53-78 <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/undp-drafting-data-protection-legislation-march-2023-443.pdf>>; Centre for Communication Governance, *Comments on Personal Data Protection Bill, 2018* (CCG 2018) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-on-the-pdp-bill-2018-along-with-comments-to-the-srikrishna-whitepaper-396.pdf>> .

³⁷ Centre for Communication Governance, *Drafting Data Protection Legislation: A Study of Regional Frameworks*, (UNDP 2023) 39-41 <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/undp-drafting-data-protection-legislation-march-2023-443.pdf>> .

processing personal data and designing their systems and controls.³⁸ In order to fulfil transparency and accountability requirements, data controllers and processors should be required to show compliance with all data protection principles such as purpose specification, collection limitation, use limitation and maintenance of data quality.

As part of transparent processing, data controllers and processors are also obligated to comply with the notice and consent principle that helps build user control over their data. This principle makes processing of personal data contingent on acquiring informed consent from the users in a fair manner by way of notice presented in an easy to understand and accessible format.³⁹ The notice should explain to users in a clear and plain language how and why their data is being processed and the legal grounds for undertaking such activities. This system allows users to hold data controllers and processors accountable and seek redressal in case of violation of their privacy or other rights provided in the data protection framework. However, it is necessary to highlight that the notice and consent mechanism in data protection frameworks has its own limitations due to concerns like consent fatigue, power asymmetry, illusion of choice, etc.⁴⁰ Hence, it is important to enforce additional accountability and transparency related norms and safeguards (as outlined in above sections) to ensure consent is not rendered meaningless due to the above-mentioned concerns.⁴¹

TRANSPARENCY IN THE DESIGN AND IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE

Transparency requires AI systems and their associated technologies to be designed and executed in a manner that allows for oversight with respect to converting their operations into intelligible outputs.⁴² The logic of decision making employed by an AI system and the steps involved in its treatment of data is often not visible or comprehensible, particularly in the case of advanced AI systems. Building transparency into such systems would require mechanisms and standards that clearly explain to users how and why their data is being processed by these systems.

³⁸ *ibid* at 37.

³⁹ Damian Clifford, Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 Yearbook of European Law 130–187 <<https://doi.org/10.1093/yel/yey004>>.

⁴⁰ Centre for Communication Governance, *Drafting Data Protection Legislation: A Study of Regional Frameworks*, (UNDP 2023) 42-44 <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/undp-drafting-data-protection-legislation-march-2023-443.pdf>>.

⁴¹ *ibid* at 44.

⁴² Stefan Larsson and Fredrik Heintz, 'Transparency in artificial intelligence' (2020) Internet Policy Review 9(2); Centre for Communication Governance, *Comments to the Department of Telecom on the Discussion Paper on the Framework for an Indian Artificial Intelligence Stack* (October, 2020) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-to-dot-on-the-discussion-paper-on-indian-ai-stack-327.pdf>>.

RECOMMENDATIONS

Tailor measures of transparency for various stages of AI design and implementation

Currently, AI algorithms operate as black boxes that make automated decisions based on machine learning over training data, and provide very little understanding of how these decisions are made, resulting in a lack of transparency. However, it is important to aim towards explaining how AI systems make decisions. While aiming for transparency in AI processes is crucial, it is important to acknowledge that a fully transparent system may not be possible.

There are two key problems with respect to transparency in AI systems.⁴³ The first is related to public perception and understanding of how AI works, which can be addressed through increased transparency during different phases of the development process. The Institute of Electrical and Electronics Engineers recommends providing varying levels of transparency to different categories of identified stakeholder groups based on their requirements. There exist various other models⁴⁴ that can be adopted to ensure categorical review of the degree of transparency offered by an AI system.

The second transparency problem is that developers may not fully understand how their own AI systems arrive at certain solutions or make logical conclusions.⁴⁵ To tackle this issue, the adoption of Model Cards has gained traction, which are short documents that accompany trained machine learning models and carry benchmarked evaluations of their application across different cultural, demographic, and intersectional groups.⁴⁶ These cards clarify the scope of AI systems and minimise their usage in unsuitable contexts. Additionally, full documentation is provided to detail the performance characteristics of AI systems and inform users of their appropriate usage contexts.

⁴³ Centre for Communication Governance, *Comments to the Department of Telecom on the Discussion Paper on the Framework for an Indian Artificial Intelligence Stack* (October, 2020) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-to-dot-on-the-discussion-paper-on-indian-ai-stack-327.pdf>>.

⁴⁴ D. Leslie, “Understanding Artificial Intelligence Ethics and Safety” (Alan Turing Institute, 2019) <https://www.turing.ac.uk/sites/default/files/2019-06/understanding_artificial_intelligence_ethics_and_safety.pdf>.

⁴⁵ Centre for Communication Governance, *Comments to the Department of Telecom on the Discussion Paper on the Framework for an Indian Artificial Intelligence Stack* (October, 2020), 57 <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-to-dot-on-the-discussion-paper-on-indian-ai-stack-327.pdf>>.

⁴⁶ *ibid*.



HUMAN OVERSIGHT IN ARTIFICIAL INTELLIGENCE

Control over the outcomes of an AI system and human oversight at different steps of the decision-making process can prevent the use of AI for unethical and harmful purposes. Human autonomy in defining the objectives of deployment of an AI system is critical. Human oversight and intelligence is also necessary to ensure that AI systems do not violate safety, ethics, and privacy considerations and cause or create harm, risks, and bias.

RECOMMENDATIONS

Contextual determination of degree of human oversight

AI systems require human oversight to varying degrees depending on the context and purpose of their deployment.⁴⁷ For instance, due to the sensitivity of the function and potential for significant impact on an individual's life, AI systems deployed in the context of the provision of government benefits, should have a high level of human oversight. Decisions made by the AI system should be reviewed by a human before being implemented. On the other hand, AI systems such as autonomous vehicles should have the ability for real time human intervention. There will be AI systems which are deployed in contexts that do not need constant human involvement but should have a mechanism in place for human review if a decision is subsequently raised for review by a user.⁴⁸

Regulatory principles can specify the circumstances and degree to which human oversight of AI systems is required. The purpose for which the system is deployed and impact it could have on individuals would be relevant factors in determining if human in the loop,⁴⁹ human on the loop,⁵⁰ or any other oversight mechanism is required. Periodic assessment frameworks of AI systems should include measures of the degree and capacity for human oversight. These assessments could be a combination of self-assessment, assessments by expert third parties and by regulatory bodies.⁵¹

⁴⁷ Centre for Communication Governance, *Comments to the Department of Telecom on the Discussion Paper on the Framework for an Indian Artificial Intelligence Stack* (October, 2020) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-to-dot-on-the-discussion-paper-on-indian-ai-stack-327.pdf>>.

⁴⁸ *ibid.*

⁴⁹ Ge Wang, “Humans in the Loop: The Design of Interactive AI Systems” *Human Centred Artificial Intelligence* (Stanford, 20 October 2019).

⁵⁰ *ibid.*

⁵¹ Centre for Communication Governance, *Comments to the Department of Telecom on the Discussion Paper on the Framework for an Indian Artificial Intelligence Stack* (October, 2020)

ACHIEVING PLATFORM ACCOUNTABILITY THROUGH MEANINGFUL TRANSPARENCY

Transparency has gained tremendous attention as a significant measure to ensure accountability of digital platforms. However, one of the challenges with transparency is that it can be used to provide information in a manner that does not benefit the recipient. It is necessary that transparency-based tools are curated in a manner that keeps local context, the type of the recipient and the end-value in mind.

RECOMMENDATIONS

Contextualise transparency measures based on audience and purpose

Using transparency to require platforms to be transparent about all their operations is ineffective as it can lead to platforms sharing excessive information that can ultimately be rendered meaningless.⁵² Transparency can also lead to platforms providing only specific pieces of information where the narrative or the image of their operations are tailored which can be misleading.⁵³ Therefore, it is crucial that when designing measures of accountability through transparency, they are tailored to the intended audience/stakeholder and purpose, in order to ensure that information provided is accessible and can be meaningfully utilised. For instance, information on why algorithms are showing a user a type of content should be provided differently than information provided to a researcher studying how advertisements are presented to a user. A researcher needs to be provided information with specificity and technical explanations of relevant algorithmic processes.

Further, transparency measures need to be contextualised to the local and social context especially in more diverse regions. Information published by platforms for users on how algorithmic systems function for any given purpose, whether curation, recommendation or ranking - should be clear and accessible, and should indicate the degree of control and redressal a user has over how they can influence these systems.⁵⁴

<<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-to-dot-on-the-discussion-paper-on-indian-ai-stack-327.pdf>>.

⁵² Robert Gorwa and Timothy Garton Ash, 'Democratic Transparency in the Platform Society' in Nate Persily and Josh Tucker (eds) *Social Media and Democracy: The State of the Field and Prospects for Reform* (Cambridge University Press 2020).

⁵³ *ibid.*

⁵⁴ Ranking Digital Rights, 'Privacy and Artificial Intelligence: Ranking Digital Rights Submission to Thematic Report on "the Right to Privacy in the Digital Age"' from UN Human Rights (May 2021) <<https://www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/Submissions/CSOs/Ranking-Digital-Rights.pdf>>.

DEVELOPING UNIFIED BEST PRACTICES ON TRANSPARENCY FOR PLATFORM ACCOUNTABILITY

Platform governance is still an area that is developing and it is becoming increasingly important to ensure convergence on guidelines and regulations. The metrics through which risks and harms are assessed continue to occur in silos across platforms and norms to address platform related concerns lack consensus and structure.

RECOMMENDATIONS

Establish a baseline for transparency through unified best practices

There are various mechanisms in which transparency can be operationalised such as transparency reporting, risk assessments, or audits. Different platforms may have incongruous interpretations of transparency measures and the various data points, metrics, and levels of accessibility. In order to achieve a uniform baseline to address platform harms, it is necessary for regulators to offer detailed guidelines and coordinate with platforms to determine unified best practices.

ACCESS FOR ALL

Principle 4

Key Recommendations for Access for All

In order to build an inclusive experiential culture for the digital world, accessibility should be built on three main fronts: access to stable infrastructure, access to data and control over it, and access to justice for all. The concept of access to technology must integrate within its design and implementation the ideas of social justice to build a just and fair digital world. Justice in the digital world, like technology, should be delivered at the doorstep, especially for marginalised and vulnerable communities engaging with technology in remote areas having weak bandwidth, low levels of literacy and poor understanding of harms.

DATA PROTECTION



Data protection frameworks should ensure that the right to access, correct and erase information, data portability as well as to object to automated processing is available to the users. Safeguards to freedom of speech and expression must be taken into consideration while exercising these rights.

Given the diverse local context of the Global Majority, it is essential to build grievance redressal mechanisms at multiple levels that are cost effective and easily accessible by users in remote areas as well as vulnerable and marginalised communities.

Capacity and efficiency of existing formal and informal justice systems should be assessed and strengthened to help build affordable and effective grievance redressal systems for the digital world.

Data protection frameworks must provide a graded approach to parental control depending on the potential risk associated with the services provided. Processing of children's data must be done in the best interest of children basis pre-defined parameters.



PLATFORM ACCOUNTABILITY

Users must be provided with sufficient control to change information that is collected, stored and used about them and to decide contours of content that is displayed. They must have easy access to grievance redressal mechanisms.

INTRODUCTION

Access as a construct has several virtues and values attached to it and can mean different things to different sets of groups, individuals, and economies. To build an inclusive experiential culture for the digital world, accessibility should be built on three main fronts: access to stable infrastructure, access to data and control over it, and access to justice for all.

Access to infrastructure has been a priority for all countries aspiring for digital transformation of their economy, society and governance models. Measures on this front have helped India expand its digital footprint to include diverse sections within the fold of the digital realm making the country home to both the second largest internet user base⁵⁵ and mobile phone market.⁵⁶ Digital transformation is praised by many quarters of the society as a tool for transforming human lives, but has simultaneously given rise to challenges and concerns. Questions around misrepresentation, misinformation, discrimination, power asymmetries and mass surveillance make a compelling case for assessing what we mean by ‘access for all’ and what the approach should be to ensure that benefits of digital transformation accrue to all sections of the society.

The concept of access to technology must integrate within its design and implementation the ideas of social justice to build a just and fair digital world. Defending harms emanating from the digital world require data protection frameworks to build principles and obligations that help secure the rights and freedoms of different kinds of users. Data protection frameworks designed to protect privacy and autonomy of all sections of the society especially of the new, inexperienced, young and vulnerable users need to ensure that users are able to exercise their right to decide their engagement with technology and have access to justice in case of violation of their rights. This translates to designing rights and freedoms that allows users to represent themselves in a manner they prefer, right to object to invisible monitoring and discrimination and the freedom to engage with automated decision making.

⁵⁵ IANS, ‘India's internet industry to reach \$5 trillion valuation by 2030: Redseer report’, (2 January 2023) <<https://economictimes.indiatimes.com/tech/technology/indias-internet-industry-to-reach-5-trillion-valuation-by-2030-redseer-report/articleshow/96676347.cms?from=mdr>>.

⁵⁶ Soutik Biswas, ‘Why internet growth has stalled in India’ (BBC, 23 January 2023) <<https://www.bbc.com/news/world-asia-india-64293857>>.

Justice in the digital world, like technology, should be delivered at the doorstep, especially for marginalised and vulnerable communities engaging with technology in remote areas having weak bandwidth, low levels of literacy and poor understanding of harms. Accessing formal justice systems is often a challenge for these kinds of users increasingly coming within the fold of the digital ecosystem. Hence, it is important to build justice systems at multiple levels that make grievance redressal easy, accessible, and cost effective.

Therefore, while designing elements of accessibility for the digital world, it is crucial to consider ground realities and lived experiences. In this submission, we look at the principle of access specifically through the lens of user access to control their data in data protection frameworks, access to grievance redressal mechanisms and the access to control over preferred content on platforms.

A key concern in the current digital ecosystem is that the users are unable to access, correct or erase data or content pertaining to themselves. Even after data is collected and processed or content is posted on the online platforms, it is important that the users have the right to access such details, modify those or erase those as it is imperative for users to be able to utilise their decision-making power as an exercise of their autonomy. A crucial aspect of ensuring such equitable access necessitates the understanding that users are not always an homogenous group and different forms of access need to be tailored based on the user's context.



EMBEDDING RIGHTS FOR MEANINGFUL ACCESS WITHIN DATA PROTECTION FRAMEWORKS

As an exercise of autonomy, the right to access in data protection provides users with the right to access (i) the data collected about them by the platform, (ii) the information regarding the manner in which their personal data is being processed and (iii) adequate information for making decisions to opt out of such data processing.⁵⁷ Whereas, the right to correction and erasure recognises the right of the users to seek correction and erasure of their data once the purpose for which it was collected/processed is met.

In the context of automated decision making, the right to access implies that users have access to meaningful information about the logic involved, purpose and

⁵⁷ Centre for Communication Governance, *Drafting Data Protection Legislation: A Study of Regional Frameworks*, (UNDP 2023) 59 <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/undp-drafting-data-protection-legislation-march-2023-443.pdf>>.

envisaged consequences of undertaking such data processing.⁵⁸ However, in data protection frameworks across jurisdictions, this right to access ‘meaningful’ information regarding automated processing and the right to object to automated processing is yet to be recognised and incorporated.

RECOMMENDATIONS

Incorporation of the Right to Access Information and Object to Automated Processing

The right to access meaningful information regarding automated-decision-making and the right to object to automated processing ought to be incorporated in data protection frameworks. Data controllers and processors should be mandated to take explicit consent before involving users in automated processing. Moreover, users must be provided with all the necessary information that helps them understand how the system makes decisions, the objective of undertaking such processing and the possible consequences. Given the potential of automated decision-making systems to have negative implications for users involved, it is imperative to allow them the freedom to opt out.⁵⁹

Data Portability for increased user control

The right to data portability ensures that the users have the right to easily obtain and transfer their personal data from one data controller to another. This right aids in creating interoperability in technical systems and fostering competition in the context of digital platforms.⁶⁰ The right to data portability operates to ensure the user’s autonomy over their personal data through greater choice and control.⁶¹

⁵⁸ EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 (27 April 2016) art 15.

⁵⁹ Centre for Communication Governance, *Drafting Data Protection Legislation: A Study of Regional Frameworks*, (UNDP 2023) 96 <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/undp-drafting-data-protection-legislation-march-2023-443.pdf>>; Centre for Communication Governance, *Comments to White Paper of the Committee of Experts on a Data Protection Framework for India* (CCG 2018) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-on-the-pdp-bill-2018-along-with-comments-to-the-srikrishna-whitepaper-396.pdf>>.

⁶⁰ Centre for Communication Governance, *Drafting Data Protection Legislation: A Study of Regional Frameworks* (UNDP 2023) 92 <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/undp-drafting-data-protection-legislation-march-2023-443.pdf>>.

⁶¹ Centre for Communication Governance, *Comments to White Paper of the Committee of Experts on a Data Protection Framework for India* (CCG 2018) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-on-the-pdp-bill-2018-along-with-comments-to-the-srikrishna-whitepaper-396.pdf>>.

Safeguards to Freedom of Speech and Expression in the Right to Correction and Erasure

While looking at the right to correction and erasure, any discontinuation of disclosure/processing of personal data should be balanced with the freedom of speech and expression, and the right to information. The evaluation of correction and erasure requests must be conducted by an independent authority empowered to evaluate the requests on a case-by-case basis.⁶²



ESTABLISH EFFECTIVE GRIEVANCE REDRESSAL MECHANISMS IN DATA PROTECTION FRAMEWORKS

Access to technological infrastructure without an understanding of tools and techniques to navigate the space safely can lead to risks and irreparable consequences for both the individual and society at large, especially for jurisdictions that are yet to develop and effect a data protection regime. Given the diverse local context of the Global Majority, it is essential to build grievance redressal mechanisms at multiple levels that are easily accessible by vulnerable and marginalised sections and to assess the capacity and efficiency of existing formal and informal justice systems to address concerns of the digital world.

RECOMMENDATIONS

Establishment of an effective and independent regulator

It is necessary to have a regulatory body which operationalises the data protection legislation and undertakes grievance redressal in order to protect the users. Such a regulatory body must be made independent from the executive since the State is one of the largest collectors and processors of personal data.⁶³ Additionally, ensuring adequate oversight mechanisms over the regulator can prevent arbitrariness in exercising of powers, undertaking cursory investigations and ignoring due process requirements. Therefore, it is important for the legislation to create rigid transparency and accountability mechanisms like regulatory review and reporting requirements.⁶⁴

⁶² Centre for Communication Governance, *Comments to the Ministry of Electronics and Information Technology on the Draft Digital Personal Data Protection Bill, 2022* (CCG 2022) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-to-meity-on-the-draft-digital-personal-data-protection-bill-2022-334.pdf>>.

⁶³ Centre for Communication Governance, *Drafting Data Protection Legislation: A Study of Regional Frameworks*, (UNDP 2023) 166-167 <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/undp-drafting-data-protection-legislation-march-2023-443.pdf>>.

⁶⁴ *ibid.*

Accessible Grievance Redressal Systems

Accessibility of a grievance redressal systems should be assessed in terms of ease and affordability of justice. Users from rural and remote areas as well as marginalised and vulnerable communities are unable to access these systems due to geographical distance and time and cost involved. The issue is further compounded due to their poor levels of general and digital literacy, lack of understanding of harms, or how these systems work. Therefore, establishing a grievance redressal mechanism whose access is limited to digital mediums or big cities would lead to exclusion and discrimination. Therefore, data protection frameworks must create a user-centric grievance redressal system at multiple levels to ensure accessibility for all kinds of users.



ADDITIONAL PROTECTION TO CHILDREN'S DATA

In any data protection framework and in the digital ecosystem as a whole, it is pertinent that children and their rights be dealt with separately due to the sensitive nature of their data and the higher risk of harm. However, the creation of a stringent data protection framework should ensure a delicate balance between data protection measures for children's data and the potential to prevent them from exercising their agency and autonomy and their access to the internet and related services.

RECOMMENDATIONS

Graded Approach to Parental Consent

In order to create a separate protection mechanism for children, a graded approach to parental consent needs to be considered while looking at children's data in data protection frameworks.⁶⁵ Through this approach, parental consent can be required depending on the potential risk associated with the services provided. This will enable children to use internet services that do not pose risks to them more freely while also ensuring their protection through parental consent as and where necessary.⁶⁶

⁶⁵ Centre for Communication Governance, *Comments to the Ministry of Electronics and Information Technology on the Draft Digital Personal Data Protection Bill, 2022* (CCG 2022) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-to-meity-on-the-draft-digital-personal-data-protection-bill-2022-334.pdf>>.

⁶⁶ Centre for Communication Governance, *Drafting Data Protection Legislation: A Study of Regional Frameworks*, (UNDP 2023) 109-111 <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/undp-drafting-data-protection-legislation-march-2023-443.pdf>>.

Best Interest of Children

The processing of children's data should be based on the best interests of the child.⁶⁷ The United Nations Convention on the Rights of the Child recognises the best interest principle to be crucial in all actions concerning children. The best interests of child users in all aspects of design of online services, would mean compliance with the principles of lawfulness, fairness and transparency. Hence, a parameter for determining the best interest for children must be incorporated in data protection frameworks.



INCREASED USER CONTROL ON PLATFORMS

The dimensions of user control inherently impact how autonomy over user privacy, behaviour and interests is respected. User control on platforms interacts very closely with data protection. Users should have the ability (i) to easily change how data is used by platforms and for what purposes, and (ii) to clearly understand what data and behaviour is being used to tailor content. To the extent that existing algorithms and platforms are capable, it is necessary to ensure that the user has both the knowledge and clarity on how they can exercise control over the manner in which decisions are made about them.

RECOMMENDATIONS

Establish mechanisms for user control over decisions made on platforms

To achieve the objectives of accessibility, creating awareness and incorporating tools of transparency on platforms can provide users with information on how algorithmic systems function. However, such measures need to be supplemented with the ability to alter aspects users do not prefer.

This necessitates offering users with sufficient control to change information that is collected, stored and used about them; decide contours of content they would like to be shown; and most importantly providing users with an easy to access grievance redressal mechanism.⁶⁸

⁶⁷ Centre for Communication Governance, *Comments to the Ministry of Electronics and Information Technology on the Draft Digital Personal Data Protection Bill, 2022* (CCG 2022) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-to-meity-on-the-draft-digital-personal-data-protection-bill-2022-334.pdf>>.

⁶⁸ Robert Gorwa and Timothy Garton Ash, 'Democratic Transparency in the Platform Society' in Nate Persily and Josh Tucker (eds) *Social Media and Democracy: The State of the Field and Prospects for Reform* (Cambridge University Press 2020).

INFORMATIONAL SELF DETERMINATION

Principle 5

Key Recommendations for Informational Self Determination

It is imperative to allow space for honest expression of oneself without being compelled to conform to majoritarian views, preferences, belief systems, and behaviours to build inclusive societies. Hence, guaranteeing the rights that further the human capabilities to self determine is a precondition to empowering individuals. Self determination is a crucial component in shaping individual development and sustaining a vivid democratic society.

DATA PROTECTION

A duty to act in the best interest of users and to build mechanisms that do not shift the onus of providing informed consent on the users must be imposed on data collectors and processors. In the era of big tech and machine learning, informed consent could be an illusion and lead to exploitation of vulnerable users. Hence, it is important to impose supplementary duties and safeguards on data controllers and processors which take into account the power imbalance between them and their users.

Need to harmonise data protection frameworks and technical standards at the international level to create a baseline level of protections and rights for empowering users in the digital world.

The right to be forgotten needs to be recognised and incorporated within data protection legislation as it seeks to empower the user to determine for themselves when, how, and to what extent information about them is communicated to others.



ARTIFICIAL INTELLIGENCE

In order to reduce bias in AI systems, the principle of inclusivity must feature at three separate levels: research and development, impact and representation. The process of development of AI systems should ensure diversity in the teams that design solutions, in the data used for training and building the AI system and in deciding the aims for deploying the AI system in society.

PLATFORM ACCOUNTABILITY

Many users continue to be unaware of how algorithmic systems on platforms present information to them, much less the capacity of these systems to influence their behaviour. Hence, general public awareness should be created around the impact of algorithmic systems, users rights, and mechanisms for redressal.

INTRODUCTION

Self-determination is a fundamental element of dignity which is a crucial component in shaping individual development and sustaining a vivid democratic society. The regime of data protection and privacy, and principles of access and transparency are some essential ‘tools’ to help build an inclusive digital world. For a societal structure to evolve inclusively, it is imperative to allow space for honest expression of oneself without being compelled to conform to majoritarian views, preferences, belief systems, and behaviours. Hence, guaranteeing the rights that further the human capabilities to self-determine is a precondition to empowering individuals.

Privacy protecting design and mechanisms for transparency and access creates avenues through which individuals can be empowered as they interact with emerging technologies. Empowerment may come in the form of regulations which will protect the rights of users or may provide specific rights to the users which will aid them in making decisions and taking actions with their best interests in mind. Self determination allows for such measures of empowerment to account for expression of diverse identities across different cultural, linguistic and geographic contexts.



EMPOWER USERS THROUGH THE ESTABLISHMENT OF DOMESTIC DATA PROTECTION FRAMEWORKS

Considering the importance of informational privacy of users, it is necessary to create domestic and international data protection laws and frameworks which protect individuals’ personal data across dimensions of use, regulate the use of such data and provide individuals with accessible remedies for any violations of their right to privacy and protection of personal data. These data protection frameworks must be created keeping the users and their rights in the centre.

RECOMMENDATIONS

Best interest of users at the heart of data protection frameworks

These frameworks need to be made with the users in focus in order to ensure it builds a digital ecosystem that empowers users. Regime built through these frameworks must equip and enable users with the ability to exercise their rights meaningfully. This can be done by mandating data collectors and processors to act in the best interest of their users and build mechanisms that do not shift the onus on the users. In the big tech and machine learning era, informed consent could be an illusion and lead to exploitation of vulnerable users. Hence it is important to impose supplementary duties and safeguards on data controllers and processors which take into account the power imbalance between them and their users. For instance, the burden of assessing whether user data is being processed in a lawful, fair, and secure manner can be shifted

away from users. Data protection frameworks can incentivise controllers and processors to adopt privacy seals, trustmarks or similar kinds of certifications to assure users that their data is being processed in accordance with adequate data protection requirements.⁶⁹ Building a practice of demonstrating compliance within the market can incentivise competitors to meet emerging standards of privacy and help instil trust in the ecosystem.

Harmonisation of data protection frameworks globally

It is also pertinent for us to recognise the need for some level of harmonisation of these data protection frameworks and technical standards at the international level to create a baseline level of protections and rights for empowering users in the digital world. Concerted efforts towards common goals require common understanding and intent.



INCORPORATE THE RIGHT TO BE FORGOTTEN IN DATA PROTECTION FRAMEWORKS

The right to access, correction and erasure and the right to object to automated processing (automated decision making) has been recognised to play a key role in embedding the principle of self-determination. These rights aim to empower users through agency over their data and digital personalities. Flowing from the right to erasure is the right to be forgotten which is integral to embedding values of privacy and autonomy. The right to be forgotten seeks to empower the users to determine for themselves when, how, and to what extent information about them is communicated to others. While this right has been recognised in Europe through the case of *Google Spain*⁷⁰ and in various other jurisdictions as well, it is yet to be recognised in other parts of the world.

RECOMMENDATIONS

Recognition of the right to be forgotten in data protection frameworks

The right to be forgotten needs to be recognised and incorporated within data protection legislation. However, due to concerns that the exercise of this right may in certain situations compromise transparency and free flow of information / press

⁶⁹ European Commission, 'Europrivacy: the first certification mechanism to ensure compliance with GDPR' (17 October 2022) <<https://digital-strategy.ec.europa.eu/en/news/europrivacy-first-certification-mechanism-ensure-compliance-gdpr>>.

⁷⁰ *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014) C-131/12 <<https://privacylibrary.ccgnlud.org/case/spain-sl-vs-agencia-espaola-de-proteccion-de-datos-aepd?searchuniqued=192070>>.

freedom, the right must come with exceptions for public figures, archiving in public interest and other major public interest goals.⁷¹



ENSURING INCLUSIVITY WITHIN AI SYSTEMS

The principle of inclusivity in AI systems features uniquely at three separate levels that include development, impact and representation. The process of development of AI systems should ensure diversity in the teams that design solutions, the training data that is used to build the AI system and in the aims of deployment of the AI system in society. The benefits of the AI system should lead to creation of impact that factors in the diversity of users and be distributed equally to all intended users, especially to sections of the population that have historically been discriminated against. Finally, inclusivity must also be ensured in the global representation of AI solutions and AI research from the Global Majority.

RECOMMENDATIONS

Minimise the impact of AI bias

Exclusion in AI systems can result from different types of bias. For example, when the data used to train an AI model reinforces or multiplies a specific socio-cultural bias, this leads to association bias. Common associations made by language translation tools associate terms like pilot and man, or flight attendant and woman, enabling social biases that exist in the real world to make their way into AI systems. There are different ways to minimise the impact of different kinds of AI bias. AI systems can be made more inclusive by ensuring a multidisciplinary approach to research and development by including social scientists, checking for potential biases in algorithms, exploring the complexities of human-machine interactions, and providing for gender equality in technical sectors.⁷² Another potential solution would be to monitor the use of AI after its release among different cultures and communities. The launch of a truly inclusive AI system would require continuous testing of datasets, for instance, specifically to examine the AI system's outputs for bias, thereby allowing for adjustments to be made to AI systems in real time.

⁷¹ Centre for Communication Governance, *Comments to White Paper of the Committee of Experts on a Data Protection Framework for India* (CCG 2018) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-on-the-pdp-bill-2018-along-with-comments-to-the-srikrishna-whitepaper-396.pdf>>.

⁷² Centre for Communication Governance, *Comments to the Department of Telecom on the Discussion Paper on the Framework for an Indian Artificial Intelligence Stack* (October, 2020) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-to-dot-on-the-discussion-paper-on-indian-ai-stack-327.pdf>>.



EMPOWER USERS ON PLATFORMS THROUGH MECHANISMS FOR USER AWARENESS

Algorithms can oftentimes operate in an unknown and unexplainable manner, even more so for end-users that do not have the capacity to make sense of what may be currently known about algorithmic functioning. As a result, many users continue to be unaware of how algorithmic systems on platforms present content to them, much less the capacity of these systems to influence their behaviour.

RECOMMENDATIONS

Increase awareness of platform harms, user control on platforms, and grievance redressal mechanisms

An area of focus needs to be centred around creating general public awareness around the potential ways algorithmic systems can impact users. Alongside, it is necessary to educate users about their rights, mechanisms for redressal, and how to operate platforms in a manner that suits their preferences.⁷³

⁷³ Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, <https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154>.

CONCLUSION

The Global Digital Compact presents an excellent opportunity to recognise the aspirations and role of diverse stakeholder groups and economies through various formats of convenings that will build an approach to digital development which is inclusive, equitable and diverse, and contemporary while upholding democratic values and the rule of law.

The principles of privacy, security, meaningful transparency, access for all and informational self determination, as detailed above, can aid in guiding future regulation and designing standards for the digital ecosystem. To weather the uncertainties and challenges of the rapidly evolving digital world requires a clear understanding of shared values, interests, and principles as well as a baseline of common lexicon, rights and technical standards to realise the UN Common Agenda.



Centre for Communication Governance

National Law University Delhi | Sector 14, Dwarka

New Delhi – 110078, India

ccgdelhi.org | privacylibrary.ccgnlud.org

Email: ccg@nludelhi.ac.in | Twitter: @CCGNLUD