Protecting Privacy in Indian Schools: Regulating AI-based Technologies' Design, Development and Deployment

BAJPAI, HARSH

Protecting Privacy in Indian Schools: Regulating AI-based Technologies' Design, Development and Deployment

HARSH BAJPAI

A Thesis submitted for the Degree

of

Doctor of Philosophy

Durham Law School

Durham University

2023

Protecting Privacy in Indian Schools: Regulating AI-based Technologies' Design, Development and Deployment.

HARSH BAJPAI

ABSTRACT

Education is one of the priority areas for the Indian government where Artificial Intelligence (AI) technologies are touted to bring digital transformation. Several Indian states have also started deploying facial recognition-enabled CCTV cameras, emotion recognition technologies, fingerprint scanners, and Radio frequency identification tags in their schools to provide personalised recommendations, ensure student's security, and predict the drop-out rate of students but also provide a 360-degree information of a student. Further, Integrating Aadhaar (digital identity card that works on biometric data) across AI technologies and learning and management systems (LMS) renders schools a 'panopticon'.

Certain technologies or systems like Aadhaar, CCTV cameras, GPS Systems, RFID tags, learning management systems are used primarily for continuous data collection, storage, and retention purposes. Though, they cannot be termed as AI technologies per se, are fundamental for the design and development of AI systems like facial, fingerprint, and emotion recognition technologies. The large amount of student data collected speedily through the former technologies is used to create an algorithm for the latter stated AI systems. Once algorithms are processed using machine learning (ML) techniques, they learn correlations between multiple datasets predicting each student's identity, their decisions, grades, learning growth, tendency to drop-out, and other behavioural characteristics. Such autonomous and repetitive collection, processing, storage, and retention of student data without an effective data protection legislation endangers student privacy.

The algorithmic predictions by AI technologies are an avatar of the data fed into the system. An AI technology is as good as the person collecting the data, processing it for a relevant and valuable output, and regularly evaluating the inputs going inside an AI model. If the person overlooks any relevant data, an AI model is prone to produce inaccurate predictions. However, the state, school administrations and parents' belief on AI technologies as a panacea to student's security and its educational development overlooks the context in which 'data practices' are

conducted. A right to privacy in an AI age is inextricably connected to said data practices where it gets ‘cooked’. Thus, a data protection legislation operating without understanding and regulating such data practices will remain ineffective in safeguarding privacy.

The thesis undergoes interdisciplinary research that enables a better understanding of the interplay of data practices of AI technologies with social practices of an Indian school, which the present Indian data protection legislation overlooks, endangering student’s privacy from designing, developing to deploying stages of an AI model. The thesis ends with laying out recommendations for the Indian legislature to frame a better legislation equipped for the AI/ML age, and Indian judiciary on how to evaluate the legality and reasonability of designing, developing, and deploying such technologies in schools.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ADM	Automated Decision Making
AI	Artificial Intelligence
CCTV	Closed Circuit Television Video
CJEU	Court of Justice of the European Union
CIDR	Central Identities Repository
CoE	Council of Europe
CPA	Consumer Protection Act
CPO	Child Protection Officer
DPA	Data Protection Authority
DPB	Data Protection Bill
DPbD	Data Protection by design
DPIAs	Data Protection Impact Assessments
DPO	Data Protection Officer
DPSP	Directive Principle of State Policy
ECHR	European Court of Human Rights
ECJ	European Court of Justice
EctHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Service
EU	European Union
FACS	Facial Action Coding System
FATE	Fairness, Accountability, Transparency, Equity
FERPA	Family Educational Rights and Privacy Act
FRS	Facial Recognition System
HEI	Higher Education Institution
LFRT/FRT	Live/Facial Recognition Technology
LMS	Learning and Management Systems
GDF	Guardian Data Fiduciaries
GDPR	General Data Protection Regulation
GPS	Global Positioning System
ICO	Information Commissioner Office
JPC	Joint Parliamentary Committee
MCE	Model Centric Explanations
MeITY	Ministry of Electronics and Information Technology
ML	Machine Learning
NEP	National Education Policy
NETF	National Educational Teaching Forum
Ofqual	Office of Qualifications and Examination Regulation
PDPB	Personal Data Protection Bill
PDS	Public Distribution System
PII	Personally Identifiable Information
RFID	Radio Frequency Identification
RTE	Right to Education
SC/SCI	Supreme Court/Supreme Court of India
SCE	Subject Centric Explanations
SDF	Significant Data Fiduciaries

SEL	Social and Emotional Learning
TOI	Times of India
UDISE	Unified District Information on School Education
UGC	University Grants Commission
UIDAI	Unique Identification Authority of India
UNCRC	United Nations Convention on Right of Child
UNHRC	United Nations Human Rights Convention
WEF	World Economic Forum

STATEMENT OF COPYRIGHT

DEDICATION

सर्वद्वारेषु देहेऽस्मिन्प्रकाश उपजायते।
ज्ञानं यदा तदा विद्याद्विवृद्धं सत्त्वमित्युत ॥

(Bhagvad Gita, Chapter 14, Verse 11)

Meaning: When all the gates of the body are illuminated by knowledge, know it to be a manifestation of the mode of goodness.

This thesis is solely dedicated to my mother (Mrs. Nidhi Bajpai) without whose love and support I would not have been able to complete this degree. I can write another thesis if I start listing the number of sacrifices, she has made for me to reach this point, but primarily pushing me even in her adversarial positions.

She is the one who not only introduced me to the world of PhD but has constantly taught me the importance of knowledge which shall bring goodness. And as stated in Bhagavad Gita, Chapter 14, Verse 16 - कर्मण: सुकृतस्याहु: सात्त्विकं निर्मलं फलम्, fruit of actions performed in goodness bestow pure results, the successful completion of this doctorate in law is a testament to it!!

I can't thank you enough.
Love You!
Thank You!!

ACKNOWLEDGEMENTS

यथा ह्येकेन चक्रेण न रथस्य गतिर्भवेत्।
एवं परुषकारेण विना दैवं न सिद्ध्यति।।

Source: Chanakya Neeti

Meaning: Just like the chariot cannot move on one wheel, similarly without determined effort and hard work one cannot attain success. It is a hard work of many to bring this thesis into light.

I would first like to thank my mother without whom I would not be submitting this thesis. From planting the seed in my brain to pursue PhD to the constant motivation throughout the program, in addition to the financial and emotional support, is the reason why I can produce this thesis. Had this support and backing not been there, I would not be where I am today. Also, gratitude to my father, and my younger brother who despite being silent, have provided an indirect emotional support through my tough times. A special thanks to my wife and her family in understanding the trade and tricks of academia and for showing patience in allowing me to get through the final couple of years. Shreya has been my friend and a great companion, loving, supporting, encouraging, entertaining, and helping me get through this agonising period in the most positive way, most importantly during Covid-19 phase, when we also met our dearest friend, Avleen!! While I was not the most delightful company, amidst all the research challenges, jobs/research rejections, weekend-less weeks, and five cups of espresso per day, both Shreya and Avleen happily tolerated my actions. Without those unfiltered chats, countless sacrifices, it would have been impossible to run through my thesis and finish writing it.

Immense gratitude to my supervisors Prof. Helen Fenwick and Dr. Eleni Frantziou for patiently reading and commenting on innumerable drafts of my thesis, while always being there for me, guiding, supporting, and encouraging me throughout the PhD journey. While giving me considerable freedom in my research direction, my supervisors always ensured that the research-outputs maintained a high standard. I would also like to thank Dr Anca Chirita and Dr Ge Chen for their insightful comments during my annual progress reviews.

I would like to additionally thank all the academic communities I have been part of during my PhD and all those contributing to my work through the various conferences, seminars, and workshops

I have attended. My special appreciation goes to Durham Law School and Durham University for helping me complete this degree and participate in all these activities. Also, a big thank you to my PGR colleagues for their support, help and encouragement, in particular, Marianna (one who literally taught me to write my PhD and conduct my viva), Oluseyi (one who always motivated me throughout weekdays and 'weekends'), Kristiyan (one always ready to sit down with friendly chats), Shivaraj (a true mentor who gave helpful learnings in my first year of PhD) and Shafquat (for long, late and liberating night library sessions).

Finally, a special thank you goes to everyone at Collingwood College who made this journey easier and those that have been my family away from home: Jonty, Lydia, Noah, Simon, and nearer to home: Satyam, Vatsal, Ayush, Gyan, Shruti. Last but not the least special thanks to my punching bags and my venting souls: Pranav, Vickey, Rushita and Rishi who have been my stress and anxiety busters, and people who I can trust my life with. This thesis is the product of all your hard work and sacrifices. Thank you, Dil se! ☺

FIRST CHAPTER

PART A – OVERVIEW OF THE THESIS

The word surveillance originates from the French verb surveiller, literally translating as 'looking over'.[1] Anthony Giddens describes surveillance as monitoring information and observing individual groups' activities by others.[2] David Lyon characterises surveillance, for the purposes of influence, control, security, or leadership, the object of centralised attention and the daily consideration of others' personal information.[3] The Directorate-General for Research (EUDGR) suggests that monitoring can be characterised as 'devices or systems which can control, track and evaluate individual movements, property, and other properties, provides a more technologically oriented concept.[4] Such concepts indicate a dynamic power inherent in any monitoring system in which one party has the means and the ability to regulate, control, or even exploit others' activities.

Monitoring is complicated and unpredictable. It can foster optimism and be empowering, satisfying, restrictive, and dictatorial. In other words, monitoring serves multiple purposes depending on the user's objective in mind. Therefore, one should not believe in technological determinism, which is defined as - an apparent belief in and reliance on control via technology irrespective of whether it is benevolent or malicious.[5] This would result in bad decision-making and over-control by those involved in policymaking. Technologies are socially constructed and embedded in a social system in which they are invented and introduced, which they cannot be separated from.[6] They relate to ideology, wealth, institutional priorities, and social inequalities. Monitoring behaviours can affect actions and can never be seen to be unbiased in their impact.[7] As warned by Martin Heidegger:

[1]David Lyon, *The search for surveillance theories* in Theorizing Surveillance (Willan 2006) 17-34.
[2]Anthony Giddens, *A Contemporary Critique of Historical Materialism*, vol 1 (Univ of California Press 1981) p 2.
[3] Supra note 1, p 20.
[4] European Union Directorate General for Research, *An Appraisal for Technology of Political Control* - Report (EUDGR 1998), Brussels.
[5]Clive Norris and Gary Armstrong, *The Maximum Surveillance Society: The Rise of CCTV*, vol 2 (Berg 1999) p 9.
[6]Torin Monahan (ed), *Surveillance and Security: Technological Politics and Power in Everyday Life* (Taylor & Francis 2006) ix-xi.
[7]Martin Heidegger, *The Question Concerning Technology* (Harper & Row 1977) p 4.

> *"Everywhere we remain unfree and chained to technology, whether we passionately affirm or deny it. But we are delivered over to it in the worst possible way when we regard it as something neutral: make us utterly blind to the essence of technology."*[8]

This thesis particularly looks at school monitoring of students. School monitoring is a by-product of many social, environmental, political, and corporate issues embodied in everyday activities. The school's overall purpose is always more than just about schooling; socialisation and moral education is also part of the school process. Social observers have long recognised the role of schools in instilling moral order and discipline in pupils.[9] By placing monitoring tools in the classrooms, they become part of the daily monotonous practice and, therefore, structured and internalised by pupils and staff as part of the pedagogical apparatus. Those supervised in a school are 'semi-captive,' and since the same person lives in the same space every day, surveillance is seen as usual, as repetitive and normalised as the colour of the walls around the classroom. However, the rapid changing nature and development of technologies means that school monitoring is seeing shifts in the ways students are monitored, actors involved in the monitoring process, type of information captured and the speed in which they are captured, all contributing to (re)shaping students' right to privacy.

Particularly the Indian state is installing digital technologies inside schools too, however, technologies inside classrooms is a relatively newer phenomenon.[10] For instance, the State of Gujarat launched facial recognition software in 2019 (details of which to be discussed in subsequent chapters)[11] for student and teachers' attendance and has geofencing technology which records the exact location of both.[12] The teachers raised privacy and trust concerns given that the data access is with the institution's principal, district-level education officer and education secretary of the state. Similarly, Telangana State Government has launched a policy programme called '*Haazaru Maasotsavam*', under which a mobile app '*T - Haazaru*' captures the details of

[8] Ibid.
[9] Samuel Bowles and Herbert Gintis, *Schooling in Capitalist America: Educational Reform and the Contradictions of Economic Life* (Haymarket Books 2011).; Michel Foucault, *Discipline and Punish: The Birth of the Prison* (Vintage 2012).
[10] Ashna Butani & Viraj Gaur, do we need CCTVs in Classrooms? Experts, Parents on Delhi Govt's New Plan, 10 Jul 2022, The Quint, Available at https://www.thequint.com/news/education/do-we-need-cctv-in-classrooms-delhi-government-schools.
[11] Ritu Sharma and Aditi Raja, "Gujarat's New System of Teacher Attendance" (September 7, 2019) Indian Express, available at: https://indianexpress.com/article/explained/explained-gujarat-new-system-of-teachers-attendance-through-face-recognition-5975585/.
[12] Ibid.

the teachers and students and measures their daily attendance.[13] The critical fear in the era of AI age is that information gathered through means of schools monitoring can be aggregated to build a full image of the personalities and actions of the students, for identification, categorisation or behavioural modification purposes.[14] Such collection of personal data and live tracking a student without consent endangers students' right to privacy. However, this is just one part of the entire privacy problem.

When a similar facial recognition software starts predicting students' attentiveness levels in the class through emotions, gestures, attitudes it creates a novel privacy issue. *First*, it increases the amount of personal data collection and processing, revealing the most intimate behaviours of a student. *Second*, the prediction by the technology is based only on the data that can be captured, overlooking the multiple contextualities associated with a particular emotion, or a gesture that cannot be captured as data points (not everything in the world is measurable), resulting in inaccurate predictions. Each child is subjected to a set parameter, often decided by the algorithm without any human in the loop. The technology overlooks the intersectional contexts that contribute to students attentiveness levels mediated along the axes of gender, class, religion, caste, place of birth, financial background, rather only focus on the changes in the moving style, a tilting of the head, facial expressions, a voice tone, and a style of speech.[15] Thus, the act of AI based prediction is based on selective measurable data points, both pre-empting and presuming whether a child is innocent, attentive, productive and other inferences. Such presumption is without student's active participation, an opportunity to understand how technology works and grievance redressal options. Thereby, such technologies pose threat to autonomy, dignity, and liberty of a person, impinging on decisional privacy of a student.

The thesis recognises that schools have the right to know some personal data about their students. For example, medical records and previous educational accomplishments are appropriate for schools to learn about, even though, in some situations, they may be considered confidential personal details. Therefore, depending on the context, data collection does not always amount to a breach of the right to privacy, rather depends on how it is processed, with

[13] Priyanka Richi, Telangana teachers express concerns over government new app to stop staff absenteeism, The News Minute, 04th Sep 2019, Available at https://www.thenewsminute.com/telangana/telangana-teachers-express-concerns-over-govts-new-app-stop-staff-absenteeism-108351.
[14] Christina P Moniodis, "*Moving from Nixon to NASA: privacy's second strand - a right to informational privacy*" (2012) 15 Yale Journal of Law & Technology 139.
[15] Pierre Bourdieu, *Outline of a Theory of Practice* (translated by R. Nice, 1977).

whom it is shared, where is it stored, and how it would be accessible. It is thereby necessary to understand the context and the underlying data practices to examine the legality, necessity, and proportionality of an AI technology in a given scenario. Understanding of such contextual settings by the state and the courts can aid them in framing a better legislation for better data protection and protect student's right to privacy.

PART B – RESEARCH QUESTIONS

Based on the above presented background, research questions can be grouped into three: a) conceptualisation of right to privacy, b) defining the context where AI technologies are designed, developed, and deployed and its impact on right to privacy, and c) inadequacies of the present data protection legislation in safeguarding students' privacy, which are as follows:

2.1. RESEARCH QUESTIONS

Question 1: Is conceptualising the Right to Privacy possible or needed? (Analysed in Chapters 3)

Question 2: What are the contours of an Indian school contextual setting and to what extent do the right to privacy violations arise due to the current use of AI technologies in that context? (Analysed in Chapter 4&5)

Question 3: In what respects do the current legislative proposals for reform fall short of addressing the right to privacy, as potentially violated in the contextual setting, and what measures would create a more satisfactory legislative regulatory agenda in that respect? (Analysed in Chapters 6 and 7).

2.2. SUB- QUESTIONS

2.2.1. CONCEPTUALISING PRIVACY

1. How does the current literature review frame privacy?
2. What are the ambiguities in the current framing?
3. How have the courts in India judicially assessed the right to privacy?
4. What framework allows us to conceptualise and evaluate right to privacy that adjusts to the changing contexts?

2.2.2. DEFINING CONTEXTUAL SETTING IN WHICH AI TECHNOLOGIES ENDANGER PRIVACY

1. How to define the contextual setting of an Indian school where AI technologies are being deployed?
2. What are the motivations and incentives of different stakeholders behind the design, development, and deployment of such technologies and how do they impact right to privacy?
3. What dangers, risks and harms does the collection, aggregation, processing, and sharing of personal data by AI technologies pose?
4. Are AI technologies blurring the line between personal and non-personal data, making individuals susceptible to further privacy risks?

2.2.3. QUESTIONS LINKED TO PROPOSALS FOR A POTENTIAL FRAMEWORK TO REGULATE AI AND PROTECT PRIVACY

1. To what extent, can it be said that there are any current policy frameworks laid down by the state Government or following any Central Government guidelines which relate to and constrain the use of AI-based technologies on privacy grounds?
2. Is there an exact division of responsibilities within the state regarding which body is responsible for collecting, storing, and securing data?
3. Does the safety and security of pupils provide convincing and legitimate grounds in principle on which to base the use of surveillance in Indian schools, taking the issue of panopticism into account?
4. How should courts evaluate or test AI technologies against the rule of law? What does comparative jurisprudence from UK and EU provides the Indian courts to perform the test of legality, necessity, and proportionality?
5. If privacy is a contextual right, is it possible to design a single framework protecting privacy in schools?
6. What can the Indian legislature learn, in terms of principles, approaches, and concepts, from other sectoral laws to adopt in improving the current framing of data protection law on privacy grounds?

PART C - THESIS STRUCTURE & ORIGINALITY

This part explains the thesis flow with a chapter breakdown. It will provide the readers with the structure of what is discussed in each chapter, leading to the conclusion that building a robust framework of AI regulation in schools is needed on privacy grounds.

Chapter 1 comprises a detailed thesis statement that provides a complete background to the research. Since the broader research area of the thesis concerns Artificial Intelligence Technologies, the chapter begins by proffering an understanding of the phrase 'Technology'. For such purposes, the chapter adopts Michel Foucault's conception of the word. This is because of the author's positive and negative conceptions of technology. The chapter provides the evolution of technology's definition as Foucault progressed in his intellectual career. The journey from '*technologies of power*' to '*technologies of the self*' helps the thesis locate the surveillance aspects associated with any technology. After associating surveillance with technology, the chapter provides an overview of the existing surveillance theories to show the different forms surveillance can take. Surveillance theories take the path from Bentham and Foucault's idea of the panopticon to Haggerty and Ericson's surveillant assemblage and end at Zuboff's theory of surveillance capitalism. The journey helps depict the distributed forms of surveillance it took with technological advancements. Post understanding technology and its surveillance abilities, the chapter traces the history of surveillance in schools. It discusses the motivations and needs for schools to foster technology development to enable surveillance. It also shows that such needs of the school can come into conflict with the right to privacy of students that needs to be balanced by courts and the state. The last section of the chapter recognises that both the legislature and courts are trapped in a failure to find a particular conception of privacy, leading to its ineffective regulation. Thus, the chapter raises multiple research questions for the following chapters to consider.

Chapter 2 represents an outcome of the analysis in the previous chapter. After laying out the various dilemmas, conflicts, and themes, the chapter synthesises the research questions. It suggests three broad questions for the thesis and their underlying sub-questions. The chapter also lays out the roadmap for the readers regarding the thesis's structure. The chapter also demonstrates the methodology used to examine the suggested research questions. The research methodology mainly uses two methods to examine the questions: comparative analysis and critical discourse analysis. Both techniques are extrapolated in the said chapter.

Chapter 3 performs the literature review on the right to privacy to analyse the various conceptualisations of privacy. The chapter uses Daniel Solove's taxonomy which proposes six different conceptions of privacy to perform such analysis. *The chapter's novelty lies* in the fact that it juxtaposes Solove's taxonomy with the Indian jurisprudence of the right to privacy. For instance, the chapter explores privacy's conception as intimacy or secrecy within the Indian court judgements which have pronounced on similar matters. Such juxtaposition is conducted to show that Indian courts have taken intentional steps to conceptualise 'privacy' according to a given context. The chapter dedicates a separate section to discussing informational and decisional privacy, the central theme of the thesis. The section shows a similar exercise of locating informational privacy within the Indian courts' jurisprudence. The chapter primarily focuses on court judgements as, until 2017, none of the Indian legislations explicitly regarded the Right to Privacy as a fundamental right. The chapter highlights a potential research question by depicting various formulations of the right to privacy. The solution to the questions comes in the third section of the chapter through Helen Nissenbaum's framework of '*Theory of Contextual Integrity*'. The said theory provides a framework to conceptualise privacy in a given setting.

Chapter 4 begins where the previous chapter ended. The chapter begins with analysing each component of Nissenbaum's framework in the Indian Context to conceptualise the Right to Privacy. The four components of the framework, namely, Context, Actors, Attributes/Information Type and Transmission Principles, are discussed in this chapter. The entire basis of Nissenbaum's theory is that Privacy can be viewed as arising in a contextual setting where different actors operate. The chapter lays out the *context* by typifying the everyday '*practices*' in an Indian school. The *actors* and *information types* are laid out using a case study of a socio-technical system called 'Aadhaar' that captures an individual's personal details. The chapter accepts that actors and, thereby, the information types keep changing with each technology. Finally, transmission principles are devoted to a separate section to show how personal data is collected, shared, and trained before deploying any AI-based technology. The chapter, in its entirety, shows that each 'practice' in a school and the 'materiality' of the technology breaches the right to privacy of an individual. *The chapter's novelty arises in* that it applies Nissenbaum's theory in a practical domain, particularly the Indian schools, for the first time. The said theory helps prove that schools are becoming one of students' most intrusive and aggressive environments, breaching their right to privacy, due to surveillance. Thus, though the chapter solves the first research question identified above, it raises the question of how privacy is breached by the operation of AI technology in the school context.

Chapter 5 introduces the readers to the socio-technical aspects of Artificial Intelligence based technologies. Though the previous chapter laid out how an AI-based technology operates, it was imperative to show the loss of the right to privacy at each step of the technology. It is done to address the second broader question stated above. *The novelty of the chapter* is to bring together the components of Nissenbaum's framework and tie it with the right to privacy. The chapter, by tying together the social practices of the school and technical aspects of the technology, proves that the right to privacy is constructed by the way data flows across actors in each context. *Another novelty of the chapter* is to show linkages between several data practices leading to data aggregation and how it blurs the boundaries between personal and non-personal data. It is important to show that collecting several data points (personal or non-personal) when aggregated produces a complete identity of an individual. Thus, the chapter ends with examining the dangers of using AI-based technologies in schools as they overlook the contextualities of a given setting.

Chapter 6 acts as a precursor to the final chapter, where the dangers of the existing legislative structure are evaluated. India has no legislation that protects an individual's informational and decisional privacy. While the Indian constitution explicitly included a right to privacy in 2017, no legislation specifies the rights of data subjects, the obligations of data controllers and the role of a regulatory institution. The chapter investigates the Data Protection Bill the Indian government has put forth to the parliament for the fourth time, as the previous versions have remained contested. The chapter highlights how the current and previous versions of the Bill ignore the contextualities of Indian society while also avoiding mimicking the UK/EU GDPR. The chapter suggests that regulation to protect the right to privacy effectively should learn lessons from Nissenbaum's theory.

Chapter 7 should be treated as the sum of all the parts as it attempts to suggest a regulatory AI agenda that protects children's right to privacy in schools. When the previous chapter shows that the upcoming data protection legislation has gaps and cannot protect from the dangers highlighted in Chapter 5, it became imperative for the thesis to produce a legislative and regulatory framework that protects privacy. The chapter performs Rule of Law and principles-based analysis to advise the Indian judiciary and legislature. The chapter uses case studies of three technologies for the rule of law analysis: CCTV cameras, fingerprinting, and emotion recognition. The chapter puts to test the said technologies against legality, necessity, and proportionality, showing that they fail each of the stages. In conducting the analysis, the chapter provides examples of how a rule

of law analysis should be done, a comparative analysis of how they are conducted by the ECtHR, acting as a guide for the Indian courts in future. The thesis adopts the FATE framework for principles-based analysis, initially developed by Microsoft researchers.[16] *The chapter's novelty lies* in adopting and developing the FATE principles in the Indian context. The thesis adopts the FATE framework allowing interdisciplinary research to be conducted in any context. The FATE framework sits well with Nissenbaum's theory as both push the researchers to look at the socio-material complexities in a context to arrive at a particular regulation. The last section of the chapter concludes by looking at other sectoral legislations in India that can guide the Indian legislature to frame its data protection law that protects the informational privacy of children in schools.

Chapter 8 concludes, in summary, as to the arguments presented in the previous chapters.

PART D - RESEARCH METHODOLOGY

All Indian states have seen an influx of AI-based technologies across sectors. For instance, New Delhi has one of the largest deployments in the country of CCTVs, with the state government announcing plans to install 1.4 lakh CCTVs across Delhi.[17] The India Railways is also setting aside Rs 3,000 crore in its 2018-19 budget to install CCTV systems across 11,000 trains and 8,500 stations.[18] Modern-age CCTV cameras use facial recognition systems that can capture fingerprints and iris information from a distance. In addition, there are fingerprint scanners, thermal scanners, RFID tags, GPS, and emotion tracking tools, leading to the capture of insurmountable data. A complex network of public and private actors controls such technologies' design, development, deployment and post-deployment. In a school context, public actors include the central and the state government, law enforcement agencies, government-funded schools and local-level municipal corporations. Private actors include private schools and their school administrations, people hired to collect data on the ground, data scientists, software engineers designing the technology, schools' security guards and technicians.

[16] FATE framework acronym stands for Fairness, Accountability, Transparency and Equity. It was first conceptualised by Microsoft researchers available at, Memarian B, Doleck T. *Fairness, Accountability, Transparency, and Ethics (FATE) in Artificial Intelligence (AI), and higher education: A systematic review*. Computers and Education: Artificial Intelligence. 2023. Also, read *Inuwa-Dutse I., FATE in AI: Towards Algorithmic Inclusivity and Accessibility*. arXiv, 2023. The discussion of FATE framework in Indian schools is discussed in the last chapter, Infra Chapter 7.

[17] India Today, July 2, 2020, Available at https://www.indiatoday.in/mail-today/story/installation-of-1-4-lakh-chinese-cctv-cameras-by-delhi-govt-sparks-row-1696032-2020-07-02.

[18] Murali, Anand, *The Big Eye: The tech is all ready for mass surveillance in India,* Factor Daily, Aug 13, 2018, Available at https://factordaily.com/face-recognition-mass-surveillance-in-india/.

Each actor participating in designing, developing, deploying, and using technology has its own incentives, motivations, biases, attitudes, and preferences regarding the building/using the technological layer. The government has a political incentive to bring efficiency in schools in terms of the educational growth of students or their safety and security. *Firmino and Duarte* show that the government aims to project efficiency to attract global capital.[19] The private actors, acting through their neoliberal interests, push the installation of emerging surveillance technologies. Such a push captures the inherently democratic nature of education and substitutes it with neoliberal governance.[20] The schools are being pushed under State power and private interests are coerced to implement technologies for imparting education. Amidst such an environment, students are stripped of their individual and collective sense of privacy. Such privacy should be considered from the point of decision-making, autonomy, liberty, dignity, and control over information.

With this brief background, the thesis begins with a documentary analysis of the right to privacy. Document analysis pushes the researcher to draw upon multiple sources of evidence to seek corroboration and their convergence.[21] Such corroboration provides credibility to the analysis presented and reduces the impact of bias in a study. *Patton* argues that triangulation, i.e., pieces of evidence from multiple documents, guards the researcher from accusations that the study's findings are based on a single method.[22] Chapter 3 conducts a documentary analysis by drawing on Solove's framework of conceptualising privacy. Solove's framework is chosen as it analyses the works of various authors and collects their conceptualisations of privacy. Such collection is then juxtaposed against the Indian court judgements and their arguments on different facets of the right to privacy. Such juxtaposition and documentary analysis lead to the finding that defining privacy is futile, as privacy depends on context.[23] *Thus, the first research question identified above is examined by adopting a document analysis methodology*.

[19] Duarte, F., Firmino, R., & Crestani, A. (2015). Urban phantasmagorias: Cinema and the immanent future of cities. *Space and Culture*, *18*(2), 132-142.
[20] Hastings, M. (2019). Neoliberalism and education. In *Oxford Research Encyclopedia of Education*.
[21] Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative research journal*, *9*(2), 27-40.
[22] Patton, M. Q. (1990). *Qualitative evaluation and research methods*. SAGE Publications, inc.
[23] Infra Chapter 3, Part A.

Due to the wide-scale deployment of technologies in schools, the thesis begins its journey to locate the right to privacy in the Indian school context. The thesis uses Helen Nissenbaum's theory of contextual integrity as a conceptual framework to define the context within which the right to privacy can be viewed as arising. The said theory is itself rooted in distinct conceptualisations of '*context*' that define it as domains, spheres of justice, institutions, or fields.[24] Such contexts are constituted of norms that regulate the actors, their roles, expectations, and limits. The present thesis blends Nissenbaum's context framework with the Digital sociology theory because the latter is not homogenous but multifarious in intermingling technology and society. Earlier studies using a digital sociology framework have demonstrated the effects of technology in a context, demonstrating its impact on identity formation and knowledge production.[25] The present thesis uses the two theories to show that students' experience surveillance due to the practices of a given context and the materiality of the technology. To reveal '*practices*', Chapter 4 lays out the Indian school context, the actors working in that context, and the Information types they collect. To lay out the '*materiality*' of the technology, the chapter uses Lehr and Ohm's AI/ML lifecycle, which provides the inner functioning as to how a given technology operates and shapes the right to privacy. Examining practices and materiality through the said theories helps to analyse the power relationships formed in a school, information asymmetries, identity formations, knowledge production and other social processes and structures.[26] Merging Nissenbaum and Lehr & Ohm's frameworks with Digital Sociology theory reflects concerns from critical philosophers like Foucault, Kant, and Habermas, who see social structures and processes as constitutive of politics, and therefore as having implications on notions such as power distribution.[27] Thus, the theories are rooted in broader social, cultural, and political contexts.[28] The merging of the theory and frameworks shows that '*materiality*' ignores the social aspects, thus creating sites of information asymmetry, loss of autonomy, dignity, liberty and absence of control over personal information, all leading to the breach of the right to privacy. *Thus, Chapters 4 & 5, in examining the second*

[24] Bourdieu Pierre & Wacquant J.D. Loic, An Invitation to Reflexive Sociology, 95-115 (1992); Walzer Michael, Spheres of Justice: A defense of Pluralism and Equality (1983).
[25] Selwyn, N., Nemorin, S., Bulfin, S., & Johnson, N. (2016). Toward a digital sociology of school. *Digital sociologies*, 147-162; van Deursen, A. J., van der Zeeuw, A., de Boer, P., Jansen, G., & van Rompay, T. (2021). Digital inequalities on the Internet of Things: differences in attitudes, material access, skills, and usage. *Information, Communication & Society*, *24*(2), 258-276.
[26] Brown, C. (2019). Critical Discourse Analysis and Information and Communication Technology in Education. In *Oxford Research Encyclopedia of Education*.
[27] Van Dijk, T. A. (2001). Multidisciplinary CDA: A plea for diversity. *Methods of critical discourse analysis*, *1*, 95-120.
[28] Weiss, G., & Wodak, R. (2003). Introduction: Theory, interdisciplinarity and critical discourse analysis. In *Critical discourse analysis: Theory and interdisciplinarity*, p.8. London: Palgrave Macmillan UK.

broader research question, utilises the Digital Sociology theory[29], Nissenbaum's framework of contextual integrity,[30] and Lehr & Ohm's AI/ML lifecycle[31] to locate a breach of the Right to Privacy at each stage of Technology's Design, Development and Deployment.

Once the thesis frames the right to privacy in a contextual setting and posits the harms emerging technologies raise, it highlights the cavities in the present legislative structure. It frames a sectoral AI regulation in the Indian context to safeguard the right to privacy. For such purposes, comparative legal research (CLR) methodology is undertaken. CLR is a systematic exposition of processes, procedures, norms, and their application in each system.[32] The subject of the thesis possessing a social dimension sits perfectly across CLR. As *Roscoe Pound* states, CLR is a comparison of systems rather than mere legal precepts.[33] CLR has a social dimension as it helps examine the legal systems and the underlying socioeconomic factors.[34] According to *Upendra Baxi,* constitution-makers globally, aim for the best constitutional design; however, the 'best' means shopping around the available models and adapting to their needs and aspirations.[35]

The present thesis carefully constructs and adopts CLR in Chapters 6 & 7. by adopting the Rule of Law and principles-based analysis in Chapter 6. Chapter 6 adopts CLR to examine the Indian data protection bill and comparing it with the UK, EU, and US legislations. Chapter 7 adopts the Rule of Law and a principles-based framework to analyse how such frameworks are utilised to adjudge privacy claims about AI-based technologies. To apply CLR, the choice of Tertium comparation is critical, i.e., in determining which aspects of the law would be compared.[36] For Chapter 6, the thesis chooses four key elements standard across global data protection legislations, namely, a) scope and objective, b) rights of data subjects, c) obligations of data controllers, and d) Consent and notice norms. After that, Chapter 7 draws lessons from different jurisdictions to adapt to the Rule of Law and a principle-based framework. Tying each of the four elements and their relationship in the school context together, both chapters adopt a functionalist study of CLR. According to Ralf Michaels, the functionalist comparative law is factual; '*it does not*

[29] Infra Chapter 4.
[30] Infra Chapter 3, Part C.
[31] Infra Chapter 5, Part A & B.
[32] Bhat, P. I. (2015). Comparative Method of Legal Research: Nature, Process and Potentiality. *Journal of the Indian Law Institute*, 147-173.
[33] Pound, R. (1936). What may we expect from comparative law? *ABAJ*, *22*, 56.
[34] Lepaulle, P. (1921). The function of comparative law. *Harv. L. Rev.*, *35*, 838.
[35] Baxi, U. (2013). Modelling "Optimal" Constitutional Design for Government Structures. *Comparative Constitutionalism in South Asia*, *28*.
[36] Supra 32, p., 163.

focus only on rules but on their effects, not on doctrines or structural arguments, but on events'.[37] Both Chapters evaluate the legislation and recommend the way forward for regulating AI technologies, consider the materiality of social practices and technologies, and merge critical discourse analysis with CLR.

[37] Michaels, R. (2006). The functional method of comparative law, pp. 272-73.

SECOND CHAPTER

DETAILED BACKGROUND TO THE THESIS

Before delving straight into the above identified research questions this chapter provides a detailed understanding of the key concepts that will come a reader's way along the rest of the chapters, i.e., a) Technology, b) Surveillance, c) School Monitoring and finally d) Right to Privacy. As the thesis will show in the subsequent chapters, the said four concepts are inextricably tied to each other. The chapter begins by **Part A** exploring the meaning of Technology and the purposes they serve. Since the present thesis focuses on technologies that run on data and its specific purpose of surveillance or monitoring, **Part B** lays down various surveillance theories and how they have evolved with the influx of AI-based technologies. **Part C** discusses how surveillance technologies reached the inner corridors of the Indian school and the underlying motives of the state behind their designing, development, and deployment. Finally, after showing that schools depict signs of all the surveillance theories discussed in Part B, **Part D** targets the thesis' central theme, i.e., the impact of AI technologies on students'/children privacy. In totality, the entire chapter provides a flavour of a) How technologies should be viewed in a context, b) Evolution of surveillance theories and its applicability in a school context, c) Reasons and motivations to monitor students in a school, particularly in India and d) Technologies impact on Right to Privacy. While this chapter provides a high-level view of the stated concepts, the subsequent chapters provide a detailed examination in the Indian context.

PART A: Understanding '*Technology*' in the Foucauldian Way

Technology is a word which appears in Foucault's lexicon frequently; however, it originates from a synonymous French word for technology, i.e., '*technique*'. Technique refers to tools, machines, procedures, and processes through an industrial lens and as "*methods and procedures for governing human beings*".[38] Fordism and Taylorism emerged as two 'technicist' principles of industrial management, only to be fine-tuned by George Friedmann to 'scientific management'.[39] With the emergence of the industrial revolution, it was clear that it led to the development of machinery and the mechanisation of social life - the '*sciences of humans*' (be it industrial

[38] Behrent, M. C. (2013). Foucault and technology. *History and Technology*, *29*(1), 54-104.
[39] Ibid, pg. 55-56.

psychology or social psychology). During the industrial revolution, Foucault placed '*technique*' in the context of the way that power relations operate in a working environment.[40] While challenging the notions of Industrial Revolution neutrality, Foucault stated that technology affects the consciousness, gestures, attitudes, and usages of one's body (for instance, Fordism, where the employers controlled, managed, supervised, and manipulated the workers).[41] Foucault also mentions in his book '*The Order of Things'* that the entire idea of the human soul is '*correlative of a certain technique of power over the body*' where scientific management techniques create the 'normalisation' of human relations and play with an individual's psyche.[42] This is synonymous with what Frederick W. Taylor testified before the House of Representatives committee:

> *"Scientific Management was not any efficient device, or a system of figuring costs of paying men, not even time study or motion study, nor any of the devices which an average man calls to mind when scientific management is spoken of. On the contrary, it is a complete mental revolution for the working man…."*[43]

Crozier posits similar thoughts in his book '*Human Engineering*' which discusses a manager's power in an organisation.[44] He explains how specific routinised procedures normalise human relations in an organisation, and discontent is treated as an abnormality. This description asserts Foucault's description of '*technique*' that gives birth to punitive power structures in which the soul of the human body gets imprisoned and oppressed.

Foucault was interested in the intellectuals who had provided a sophisticated account of '*humanism*'[45] using theories that go back to Immanuel Kant's Transcendental Idealism, opined in his book '*Critique of Pure Reason*'[46] and Jean-Paul Sartre's existentialism in his book

[40] Fenech, M., & Sumsion, J. (2007). Early childhood teachers and regulation: Complicating power relations using a Foucauldian lens. *Contemporary Issues in Early Childhood*, *8*(2), 109-122.
[41] An intersection of economic expansion and technological progress engaging in mass production is often studied in the context of working conditions, production - consumption. Herein, '*Fordism'* invokes readers to look at this concept from an angle of technical/technological management and production of docile bodies because of constant supervision/surveillance.
[42] Supra 10, p, 57.
[43] Daniel Nelson, "Scientific Management in Retrospect" in A Mental Revolution: Scientific Management Since Taylor (Ohio State University Press, Columbus, OH 1992) 5-39.
[44] Supra 10, p, 57-58.
[45] Michael C. Behrent, "Foucault and Technology" (2013) 29 History and Technology 54-104.Norman Kemp Smith, Immanuel Kant's Critique of Pure Reason (Read Books Ltd 2011).
[46] Smith, Norman Kemp. *Immanuel Kant's critique of pure reason*. Read Books Ltd, 2011.

'*Existentialism as a Humanism*'.[47] Both theories emphasise the existence of individuals in a society as free and responsible agents. However, the concern with technology was that it dehumanises an individual in which the body is broken into datasets enabling its measurement, sorting, and profiling. This violates all capacities by which a human lives life as stipulated by Martha Nussbaum - capacities for life, health, imagination, emotions, practical reason, affiliation, and self-respect.[48] Thus, Foucault observes the industrial revolution technologies through the lens of human sciences and the way that such techniques exacerbate the severity of the harm, leading to the curtailment of human freedom.

The above understanding of Foucault's idea of technology can be squarely placed onto AI technologies running on biometrics, or other personal data. AI technology shows that they go beyond the industrial revolution technologies in terms of the *speed* at which they perform, the *intensity* with which they monitor and the *levels of access* to data they possess. There are motivations and controls of several stakeholders that enable the design, development, and deployment of surveillance technologies, as demonstrated in the subsequent chapters.[49] It is necessary to visibilise the involved stakeholders and the context where AI technologies are designed and deployed to understand what control over personal information a data subject or a data controller has. The said control will dictate the usage of the technology, the risks and harms they pose to right to privacy and the nature of grievance redressal needed. Thus, to evaluate AI technologies impact on privacy, it is necessary to examine the relationship between the observer and the observed, after all it's a human science.

PART B: Understanding Surveillance Theories: Organisation, Monitoring and Control of Minds

Surveillance is a dynamic concept continuously changing with increasing awareness and influx of Information and Communication technologies. The spatial distribution, motivations for surveillance and the nature of the subjects of surveillance have also evolved. As David Lyon states, surveillance has two core purposes - monitoring and caring. The subjects are watched with a clear purpose of imparting discipline within a set structure of norms and, at the same time

[47] Jean-Paul Sartre and Philip Mairet, Existentialism and Humanism (Methuen 1960).
[48] Martha C. Nussbaum, Creating Capabilities: The Human Development Approach (Harvard University Press 2011).
[49] Infra, Chapter 4, Part B, 2.2., pg. 113.

caring for the said subject.[50] Herein, schools fall perfectly into the environment where children can be subject to surveillance for caring and discipline without fearing a backlash from either students or guardians. Schools have always been a focus of importance for educators and academicians to use the metaphor of the '*Panopticon*' as a helpful way of understanding the disciplinary mechanisms and power relations in schools.[51] Schooling is viewed as emancipatory[52] and authoritarian,[53] where surveillance is based on fear or presumption of fear, risk, corporatism, and adoption of zero tolerance pedagogy.

This has led to many surveillance studies - a multidisciplinary field studying surveillance in various contexts and disciplines like urban planning, policing etc. - and can be thematically divided into three categories, which will be explained in turn. The following surveillance theories are discussed to show their relevance even in a modern school monitoring context. They aid our understanding of the relationship and the power structures between the watcher and the watched, and its impact on several aspects of right to privacy.

- The first point of departure is the Jeremy Bentham architectural model of a prison which formed the edifice of the Panopticism theory of Michel Foucault.[54]
- The second point of departure is the post-panoptic theories, including Deleuze and Guattari's *Control Society*[55] and Haggerty and Ericsson's *Surveillant Assemblage*.[56]
- The third point of departure is not a new model on its own but a combination of the other two approaches or a branch of already established Surveillance theories, but much more relevant in the age of artificial intelligence and biometric technologies, including Shoshana Zuboff's *surveillance capitalism*.[57]

[50]David Lyon, "The Search for Surveillance Theories" in David Lyon (ed), Theorising Surveillance: The Panopticon and Beyond (2006) 3-20.
[51] David Lyon, "Surveillance as Social Sorting: Computer Codes and Mobile Bodies" in David Lyon (ed), Surveillance as Social Sorting: Privacy, Risk, & Digital Discrimination (Routledge 2003) 13–28.
[52] Émile Durkheim, "Moral Education: A Study in the Theory and Application of the Sociology of Education" (1925).
[53]Supra note 9.
[54] Lyon, D. (2006). The search for surveillance theories. *Theorizing surveillance*, 3-20.
[55] Celis Bueno, Claudio. "The face revisited: Using Deleuze and Guattari to explore the politics of algorithmic face recognition." Theory, Culture & Society 37, no. 1 (2020): 73-91.
[56] Haggerty, K.D. and Ericson, R.V., 2000. The surveillant assemblage. *The British journal of sociology*, *51*(4), pp.605-622.
[57] Zuboff, S., 2019. *The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019*. Profile books.

As the chapter will demonstrate, the current surveillance practices in Indian schools share features of all the below discussed normative theories. While Part B of this chapter provides a descriptive account of the theories, the chapters ahead show their relationship with Indian schools specifically, and how breaches of the right to privacy occur.[58]

2.1. BENTHAM'S PANOPTIC MODEL

Surveillance Studies can be traced back to Bentham's conception of the prison panopticon, which became widely popular when adapted by Michel Foucault.[59] Foucault described the prison panopticon as an institution with power dynamics between the prisoners and the jail guards due to constant monitoring by the latter. Anne Brunnon-Ernst further deconstructed panoptical structures by Bentham into four categories.[60] Besides the well-known prison panopticon, there are other panoptical institutions designed to serve the social issues of those times, like the Chrestomathic Panopticon (panopticon-shaped day school with a teacher keeping an eye on students),[61] Pauper Panopticon[62] (designed for housing of indigents) and the Constitutional Panopticon (in which the state is not watching the citizen but citizens are watching the few, thus also called as inverted panopticon).[63] It is imperative to outline the characteristics of each panopticon, as it would enable us to examine surveillance in schools through those lenses and consider contrasts between the features of the different panopticons.

The *Prison panopticon* has guards at the center, with subjects in their own cells. The guard's omnipresence is the only 'utterly dark spot' in the ever-transparent design of the cell.[64] The panoptic structure creates an illusion in the subject's minds that they are constantly being watched. However, Bentham's notion of the panoptic structure is not continuous supervision of the subject, but rather an internalisation of discipline to obviate the need for observation and

[58] Infra Chapter 4, Part C, pg. 119.
[59] Jeremy Bentham, *Panopticon, or the Inspection House*, vol 2 (1791). For Foucault's adaptation of Bentham's panopticon, refer to Supra 25, p., 10-11.
[60] Anna Brunon-Ernst, "*Deconstructing Panopticism into the Plural Panopticons*" in Beyond Foucault (Routledge 2016) 33-58.
[61] Jeremy Bentham, "*Chrestomathia*" (1816) The Works of Jeremy Bentham, Vol. Eight, reprinted, New York 1-191 (1962).
[62] Jeremy Bentham, "*Outline of a Work entitled Pauper Management*" in The Works of Jeremy Bentham, 1838-1843 (1797).
[63] Jeremy Bentham, *The Collected Works of Jeremy Bentham: Constitutional Code: Volume I*, vol 1 (The Rosen Publishing Group 1983).
[64] Jeremy Bentham and Miran Božovič, *The Panopticon Writings* (Verso Trade 1995).

punishment.[65] He believed in reforming prisoners or indigents to achieve his utilitarian philosophy - 'greater good for greater happiness'.

As the name suggests, the *Pauper panopticon* housed paupers in a workhouse who voluntarily submitted themselves to such spaces. Their poverty was due to increasing bad debt, crop failure and the French declaration of war, which decimated public and private wealth. Paupers were given food, housing, and a nominal stipend for their labour. However, just like prisoners, they were supervised not only by the workhouse security guards, but also by the older paupers through bookkeeping and other rules. The space was distinct to prison as paupers enjoyed limited privacy - example, at times of marital sex, sleep - and thereby experienced only an intermittent gaze.

The *Chrestomathic panopticon* was a school in the design of a panoptic where a master supervised 600 pupils per room, and the former cannot be seen. Bell's[66] and Lancaster's Monitorial system[67] inspired the school design in which docile bodies moved in an organised and disciplinary way akin to product lines at manufacturing sites. There is constant supervision by masters, aided by monitors; however, only when the child is in school. The time-limited gaze distinguishes the Chrestomathic from the prison and pauper panoptic structure. The schools were designed to be militaristic in style with the spatial and temporal organisation of the pupil and the classroom, performing specific tasks in a time-bound manner while getting educated. This required constant supervision, precision, discipline, and organisation, resulting in bodily control of the pupils.

The *Constitutional panopticon* is the least panoptic of all, or, as some scholars say, is an inverted panopticon.[68] It lacks any enclosed space or a centralised structure. Instead, the citizens keep an eye over elected officials in the administration - for example, by way of print or digital media - to maintain transparency and accountability. The act of watching is temporal and is reduced considerably in contrast to other panoptic structures. It is like the Chrestomathic panopticon in

[65] Galič M, Timan T, Koops BJ. Bentham, Deleuze and beyond: An overview of surveillance theories from the panopticon to participation. Philosophy & Technology. 2017 Mar 30, 9-37.
[66]Andrew Bell, *An Experiment in Education, made at the Male Asylum at Egmore, Near Madras: Suggesting a System by Which a School or Family May Teach Itself Under the Superintendence of the Master Or Parent* (Cadell and Davies 1805).
[67] Joseph Lancaster, *Improvements in Education, as it Respects the Industrious Classes of the Community: Containing Among Other Important Particulars, an Account of the Institution for the Education of One Thousand Poor Children*, Borough Road, Southwark; and of the New System of Education on which it is conducted (Collins and Perkins 1807).
[68]James Semple, "*Bentham's Haunted House*" (1987) 11 The Bentham Newsletter 35-44.

that government officers are watched and thereby accountable for only 'public duties' - akin to children being watched only when they are in school.

The Chrestomathic panopticon looks synonymous with the purposes of this thesis because it is set in a school setting. However, as the thesis progresses, the modern-day school would also resemble the prison panopticon. It is primarily because of the increased availability of emerging technologies and their reach through which children can be monitored without their consent. The panopticon concept has evolved into '*governmentality*' - Foucauldian thought of the exercise of power over a particular population through institutions, processes, and procedures to manage, organise and produce docile bodies, resulting in monitoring being a continuous process, irrespective of one's location. [69]

2.2. THE FOUCAULT PANOPTICISM MODEL

The theoretical and social importance of surveillance in contemporary culture is described by Foucault using an essential metaphor - the *Panopticon*.[70] The Panopticon is an architectural model for Foucault's study of disciplinary control, and the idea has interminably embedded itself in the minds of surveillance scholars. The Panopticon is a circular structure with a central observation tower that allows the jailor to observe detainees continuously. The Panopticon makes prisoners permanently observable, coercing them to be in an environment of persistent fear of any non-conformity bringing punishment, thus intensifying the interference into an individual's physical and mental spaces. The continuous fear of non-conformity also instills control and discipline in the prisoners, rendering anticipatory conformity over a period. Foucault was influenced by the architectural nature of the Panopticon to explain the anatomy of surveillance, which he called '*Panopticism*'. He saw in it a control system reduced to its basic shape.[71] In a panopticon, power is not exercised by blunt coercion but is internalised and transmitted to the subjects. Panopticism creates a state of consciousness and perceptual recognition that ensures that 'control' works automatically.[72] For Foucault, the capacity engraved in the Panopticon systems reflected the change from repression to disciplinary control mechanisms:

[69] Michel Foucault, *The Foucault Effect: Studies in Governmentality* (University of Chicago Press 1991).
[70] Clive Norris, "*From Personal to Digital: CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control*" in Surveillance as Social Sorting (Routledge 2005) 263-295.
[71] Supra note 30, p. 205.
[72] Ibid., p. 201.

> *"There is no need for arms, physical violence, or material constraints. Just a gaze. An inspecting gaze, a gaze which each individual under its weight will end by internalising to the point that he is his overseer, each individual thus exercising this surveillance over and against himself. A superb formula: power exercised continuously and for what turns out to be minimal cost."*[73]

According to Foucault's model, the technology's panoptic gaze seeps into individual lives, minds, daily activities and learning processes, which gives rise to a disciplinary society. In a panopticon, the gazing is pervasive and ubiquitous, primarily to maintain discipline, which gives power to the watcher.[74] Foucault distinguishes between earlier feudal societies (in which the decree of the king has validity and sole power) and a disciplinary society (in which the power is dispersed across society, but institutions exercise authority and converge through state-like prisons, medical establishments, schools etc.).[75] Thus, the disciplinary societies are the architecture of surveillance through perceived democratic institutions, including schools.

The above discussion raises the question of whether schools can be considered panoptic. The view of schools by scholars as panoptic is becoming increasingly popular.[76] Schools may appear disturbingly panoptic[77] or gazeful,[78] but Michael Gallagher argues that the school cannot be considered panoptic because of the discontinuous monitoring.[79] The panoptic nature of schools is limited to when children are in a classroom or the school territory. Nevertheless, at least for a limited period, schools can be termed as panoptic because of the actual power lying with the watcher (be it teacher, principal, class monitors or security guards or even parents/guardian), creating a persistent sense of fear by their mere presence rather than via its enforcement methods

---

[73] Ibid, p.55.
[74]Gilles Deleuze, "*Postscript on the Societies of Control*" (1992) 59 October 3-7.
[75] Maritza Valverde, "*Police, Sovereignty, and Law: Foucauldian Reflections*" in Police and the Liberal State (Stanford University Press 2008).
[76] Laura Azzarito, "*The Panopticon of Physical Education: Pretty, Active and Ideally White*" (2009) 14 Physical Education and Sport Pedagogy 19-39. Holly Blackford, "*Playground Panopticism: Ring-Around-the-Children, a Pocketful of Women*" (2004) 11 Childhood 227-249. Damien Page, "*The Abolition of the General Teaching Council for England and the Future of Teacher Discipline*" (2013) 28 Journal of Education Policy 231-246. Jane Perryman, "*Panoptic Performativity and School Inspection Regimes: Disciplinary Mechanisms and Life Under Special Measures*" (2006) 21 Journal of Education Policy 147-161.
[77] Micheal Gallagher, "*Are Schools Panoptic?*" (2010) 7 Surveillance & Society 262-272.
[78]Trevor Welland, "*Living in the 'Empire of the Gaze': Time, Enclosure and Surveillance in a Theological College*" (2001) 49 The Sociological Review 117-135.
[79] Ibid, p. 120.

of punishment. Thus, panopticism is more a matter of strength and obscurity than absoluteness. For instance, CCTV cameras deployed inside classrooms are a contemporary example, as children do not need to know whether it is functioning; the presence inevitably affects behaviour.[80] Therefore, the presence of technologies on a school campus, be it for a limited period, makes the 'watched' (children) passive subjects in a power structure outside their control. The next set of chapters will take the conversation forward by arguing that schools can be termed panoptic due to technological advancements like Artificial Intelligence-based applications: biometric technologies that surveil students even when the child has left the school territory.

Foucault defines a school as a controlled and compliant workforce system, taking the argument back to disciplinary society.[81] To achieve subjugation and compliance to work, a disciplinary spirit in an organisation based on learning is required, which a school provides.[82] Also, society seeks due to its own requirements to produce disciplined children who can later work professionally and contribute to its advancement. Technologies, or the watcher in the case of a panopticon, simply assist in the said goal of the society without understanding the power disparity, information asymmetry and lack of privacy it brings. In this sense, Foucault's contribution to drawing up new power anatomy during the 17th and 18th centuries is laudatory:

> *"Discipline is a type of power, a modality for its exercise, comprising a whole set of instruments, techniques, procedures, levels of application, targets; it is a physics or anatomy of power, a technology."*[83]

In a panopticon, the subjects are aware of continuous surveillance, but we live in a digital age where covert surveillance is the norm. Covert surveillance deceives the subject of an existing environment, unknowingly resulting in data protection and privacy breaches.[84] Norris argues that covert surveillance is, also in effect, '*panoptic*'. The nature of contemporary technologies has allowed the schools to create a panoptic effect without letting the 'watched' know of the presence of any technology. For instance, cameras or biometric scanners can be installed inconspicuously

[80] Martin Gill and Karryn Loveday, "*What Do Offenders Think About CCTV?*" (2003) 5 Crime Prevention and Community Safety 17-25.
[81] Michel Foucault, *Discipline and Punish: The Birth of a Prison* (A. Sheridan trans., Penguin Books 1977) 172.
[82] Supra note 28, p. 47.
[83] Supra note 30, pp. 215-216.
[84] Stanley I. Benn, "*Privacy, Freedom, and Respect for Persons*" in Privacy and Personality (Routledge 2017) 1-26.

without changing the architecture of the school setting (they can be thought of as highway speed traps that are not always visible). Thus, Panopticism should not be viewed just as an ability to observe those within a field of vision; rather, emerging technologies exhibit the ability to monitor the entire '*assemblage*' (the term further described in the next sub-section).

Supervision of every instance or an illusion of it in a disciplinary society differentiates, compares, hierarchises, excludes people and normalises surveillance. Foucault explains:

> *"The power of the Panopticon is embodied in its ability to subject all to a surveillance gaze and to link observation to a named subject through an individualised record, which can then be used for identification, bureaucratic codification, and eventual classification".*[85]

Such identification, codification, and classification can be seen in today's Indian schools too, as described in detail, in Chapter 4. [86]

The next section takes inspiration from the Foucauldian panopticon theory but advances the notion by fitting it into contemporary society. In the panoptic world, surveillance minimises disorderly behaviour and brings discipline to the setting. However, surveillance's location, intensity, timing, motivation, and incentives are changing in the post-panoptic world.

2.3. DELEUZE AND GUATTARI '*CONTROL SOCIETY*' AND HAGGERTY AND ERICSON'S 'SURVEILLANT ASSEMBLAGE': SHIFT FROM PANOPTICON TO POST-PANOPTIC PEDAGOGY

Deleuze and Guattari draw constellations to explain the theory of assemblages and different heterogeneous elements that constitute them. The assemblage includes three stages - a) composing different bodies, elements, and concepts, called *'coding'*; b) arranging hierarchical bodies, called '*stratification';* and c) ordering the bodies, called '*territorialisation'*.[87] The *Deleuzian* theory of Assemblage signifies systems of control that form a network and a network whose constituents interact to take actions and yield results. Such a system of control can be interpreted

[85] Supra note 33, p.256.
[86] Infra, Chapter 4, Part B-C.
[87] Deleuze, Gilles and Guattari, Felix, *A Thousand Plateaus: Capitalism and Schizophrenia*. Translation and Foreword by Brian Massumi. Minneapolis: University of Minnesota Press. This book was originally published as Mille Plateaux, volume 2 of *Capitalisme et Schizophrenie* 1980 by Les Editions de Minuit, Paris, 1987, pg. 40.

as a government that functions constitutively with numerous networks, each having its process, rationality, and control, eventually territorialising. The said numerous networks can be interpreted as a set of private institutions that incentivise or motivate the government to procure technologies that promise to transform the delivery of social services like education. Such collusion of public and private actors enables the designing, developing, and deploying of AI-based technologies, resulting in the corporatisation of educational institutions and stratification of children.

The post-panoptic pedagogy has shifted from the Foucauldian notion of governmentality, i.e., from a *'disciplining society'* to a *'control society'*. The transformation is primarily due to the rise of market capitalism and globalisation, which in turn aids the corporatisation of the institutions, for, say, schools. The increased usage of school security equipment like CCTV cameras, biometric systems, metal detectors etc., is primarily due to people's perceptions of the effectiveness of these technologies and simultaneous coercion & inducement to install them. The control society presents itself as providing a sense of liberty and freedom, uniquely different from enclosed structures like prisons or schools. The visible gaze is absent (like a guard) and gives us a sense of freedom, but the individual is increasingly tracked. The gaze is omnipresent, unlike in Foucauldian society, where the gaze was present only within enclosed spaces. The control society furthers the normalisation of surveillance, masked from resistance due to its invisible nature. Thus, the control society signifies that children are being surveilled inside classrooms, schools, and outside.

In contrast to a disciplined society (where individuals are observed, trained, and disciplined, resulting in the production of docile humans), here specific individuals are not the target of the watcher, nor is there any central observatory tower. In a disciplined society, there is a precise target or a set of populations on which the scrutiny is conducted. However, everyone is under surveillance in a controlled society, regardless of reason or motivation. Deleuze dubs it the modulation of systems and institutions happening in opaque and invisible surveillance networks, unlike in Foucault's world, where discipline is a visible power, although involuntarily imposed. Deleuze breaks the notion of 'individual' etymologically (in = not + dividual = divisible), i.e., the individual is fragmented in a control society.[88] The real bodies serve no purpose in the Deleuzian society - rather, the bodies have transformed into data banks. This marks a fundamental shift

[88] D'Amato, P. (2019). Simondon and the Technologies of Control: On the Individuation of the Dividual. *Culture, Theory and Critique*, *60*(3-4), 300-314.

from the centralised institution of power to rhizomatic opaque networks[89] (as Deleuze describes Rhizomes that grow through an interconnected vertical root system but are not visible to the naked eye), i.e., in multidisciplinary ways and forms, making biopower (control over bodies and its subjugation) much more effective.[90]

Panopticon's design is limited to the institution's territory, whereas surveillance in a control society traverses nation-state boundaries. Surveillant assemblage can capture the institutions, systems and processes that enable sharing of data across & outside institutions and how they aggregate, sort and profile individuals.[91] In the case of schools, collection of data like attendance records, personally identifiable information of a student like a name, address, contact information, religion, caste, date of birth, exam records and grades, global positioning system in the bus, Radio-Frequency Identification Cards (RFID), not only leads to individual subjectification but also provides the power to the watcher to control the data flows. In modern society, such control over individual data has led to what *Roger Clarke* calls '*dataveillance*'.[92]

The said 'dataveillance' can make surveillance global when the data is transferred to the assemblages of countries, regions, agencies, and authorities, making surveillance more complex and extraterritorial. Lyon refers to such assemblages as 'leaky containers', assembling the information in centralised repositories for security purposes, persistently posing a risk to data protection and privacy rights.[93] The situation is further aggravated in children incapable of understanding such complex assemblages and legally incapable of taking decisions over their data usage. Thus, surveillance on students inside classrooms or schools needs to be examined along with surveillance outside the school territory, as contemporary surveillance technologies have expanded the role of markets and the interventionist state, both (re)formulating the freedoms an individual can enjoy. Haggerty and Ericsson, while noting the societal transformation, apply

[89]Nikolas Rose, *Powers of Freedom: Reframing Political Thought* (Cambridge University Press 1999). Roger Clarke and Graham Greenleaf, "*Dataveillance Regulation: A Research Framework*" (2017) 25 JL Inf. & Sci. 104.
[90] Supra 26, p. 75.
[91] Thomas, P. N. (2019). "*The Expansion of Politics as Control: Surveillance in India*" in The politics of digital India: Between local compulsions and transnational pressures. Oxford University Press.
[92]Roger Clarke and Graham Greenleaf, "*Dataveillance Regulation: A Research Framework*" (2017) 25 JL Inf. & Sci. 104
[93]David Lyon, Surveillance Society: Monitoring Everyday Life (McGraw-Hill Education (UK) 2001).

the assemblage theory to surveillance. Thus, *Haggerty and Ericson's* 'Surveillant assemblage' theory is based on *Deleuze and Guattari's* theory of 'assemblages'.[94]

The assemblage theory can also be applied to the surveillance concept as it comes into effect with the formation of modern society. *Gidden* views surveillance because of modernity rather than capitalism:

> *"Surveillance as the mobilising of administrative power - through the storage of control and personal information - is the primary means of the concentration of authoritative resources involved in the formation of the nation-state".*[95]

Those sympathetic towards surveillance offer that it is meant to watch over and relate to the concept of guardianship.[96] However, seeing surveillance as guardianship is a paternalistic conception that undervalues autonomy over data collection and other surveillance decisions. It also fails to note the power disparity and information asymmetry between the 'watcher' and the 'watched'.

The surveillance process can be termed as an 'assemblage' that operates through multiple actors at multiple sites and forms an aggregated web of systems were locating a chain of authority for liability is complex. It means that surveillance does not work but is embodied in networks and generated and reproduced for some means to achieve, like discipline or security. In this sense, assemblage relates to the consequentialities of panopticism, i.e. creating a disciplinary society for ordering and security.[97] However, the current state of surveillance is more fluid, malleable and de-territorialising, ever-flowing in the information society - just like a rhizome.[98] The panoptic society has funnelled its characteristics into the broader society, which *Galloway* describes as a

[94]Gilles Deleuze and Félix Guattari, A Thousand Plateaus: Capitalism and Schizophrenia (Bloomsbury Publishing 1988).
[95]Colin Campbell, The Coalescent State: Assemblages of Surveillance and Public Policy (2020).
[96]William Bogard, "*Surveillance Assemblages and Lines of Flight*" in Theorizing Surveillance (Willan 2006) 111-136.
[97] Michel Foucault explains the concept of surveillance for security through 'biopolitics', which means management of the entire population in particular territorial configurations. Michel Foucault, Security, Territory, Population (2007).
[98] David Murakami, "*What is Global Surveillance? Towards a Relational Political Economy of the Global Surveillant Assemblage*" (2013) 49 Geoforum 317-326.

combination of tight vertical control and horizontal freedom offering a distributed and networked control society.[99]

The theory moves away from panopticism, and the disciplinary roots embedded within to a mechanism of *'social integration'* whereby monitoring and profiling habits, actions and behaviour, and consumer profiles are constructed. *Haggerty and Ericson* term it as - *'disappearance of disappearance'* - where individuals do not have a right to anonymity and a sense of personal freedom. The main aim in a post-panoptic world is not to create a docile body but to control the data flow. *Haggerty and Ericson* stipulate this as a change in the '*surplus value*' concept associated with Marxism. Earlier, the surplus value was labour-oriented, in which the powerful set the means of production and capitalised on the labour's surplus work. However, today every interaction and transaction between institutions or individuals, or between them, is recorded for market purposes and not limited only to providing security.

A variety of technologies, together with state and non-state institutions, constitute an assemblage under which a child is under constant scrutiny in today's Indian schools. The said scrutiny is not only limited to the purpose of imparting discipline or learning progress but continuous data aggregation and data flows, including the monitoring of health profiles, behavioural insights, Internet use, online and offline communication patterns and political and religious inclinations of a child. Thus, in the post-panoptic world, surveillance has acquired a voyeuristic value that transcends the child's classroom, rather enters new forms of 'data networks' and 'data territories' (like rhizomes), further exacerbating the loss of control over one's own information.

2.4. SHOSHANA ZUBOFF: SURVEILLANCE CAPITALISM

Examining surveillance through the lens of capitalism is not new. Marx himself saw surveillance to exercise domination over the labour force and ensure the thriving of capitalist economy through the blood and sweat of the working class. However, during the industrial revolution, surveillance was only at the stage of capital production, i.e., workplace and workforce surveillance. Now, it is extended to the stage of capital circulation, i.e., consumer surveillance or surveillance of competitors. As Maurizio Lazzarato maintains:

[99]Alexander R. Galloway, Protocol: How Control Exists after Decentralization (MIT Press 2004).

> *"Rather than ensuring the surveillance of inner workings of the production process and the supervision of the markets of raw materials (labour included), business is focused on the terrain outside of the production process: sales and the relationship with the consumer".*[100]

In the surveillance age, labour is still present, but it is not working under the powerful; instead, it is the raw material for the institutions. In the Information economy, the human bodies are both producers of data as well as consumers of digital services. *Alvin Toffler* introduces a term for blurring the line between producers and consumers - '*prosumer*'.[101] In the case of a child under surveillance in schools, the child is using the services of an institution to gain knowledge. In exchange, its behaviour, emotions, and records are monitored, supposedly to ensure that the child is disciplined, protected from harm or to monitor its learning progress, which ends up in the child's sorting and profiling. *Fuchs* argues that "the combination of surveillance and prosumption is at the heart of data accumulation in the information age".[102] The market institutions herd, coach, and modify the behaviour of consumers to achieve their commercial outcomes - which Zuboff refers to '*Instrumentarian Power*'.[103] Such power is different from totalitarian power, as in the latter, the institutions change the souls of human beings. However, as Zuboff shows in her book '*Surveillance Capitalism*', Instrumentarian power can persuade, coerce, allure, and excite the institutions to exert totalitarian power.[104] It means that school authorities (institutions) per se might not be motivated to use surveillance technologies until the market forces (Instrument) bait them into purchasing their technology; however, this cannot be generalised and depends upon each transaction.

Oscar Gandy combines surveillance and prosumption into what he calls a '*panoptic sort*':

> *"The panoptic sort is the complex technology that involves the collection, processing and sharing of information about individuals and groups that are generated through their daily*

[100]Maurizio Lazzarato, "*Immaterial Labour*" (1996) Contemporary Marxist Theory 77.
[101]Alvin Toffler, The Third Wave, vol 484 (Bantam Books 1980) 267.
[102] Christian Fuchs, "*Web 2.0, Prosumption, and Surveillance*" (2011) 8 Surveillance & Society, p. 296. Nicole S. Cohen, "*The Valorization of Surveillance: Towards a Political Economy of Facebook*" (2008) 22 Democratic Communiqué 5-5.
[103]Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (Public Affairs 2019).
[104] Ibid, p. 34.

> *lives as citizens, employees and consumers and is used to coordinate and control their access to the goods and services that define life in the modern capitalist economy".*[105]

Zuboff argues that Surveillance Capitalism cannot be equated to algorithms, Artificial Intelligence or Machine Learning, but it does rely on them to exert its force. Surveillance capitalism is an economic logic where algorithms are a tool and data accumulation, and commodification are a consequence. The theory of assemblage and surveillance capitalism makes the network of actors, institutions, and processes transparent; however, the latter is an advanced version of the former. While the assemblage theory provides a framework for locating a variety of stakeholders involved in surveillance, surveillance capitalism identifies specific market forces involved in 'datafication' while also identifying their reasons and logic. So, while assemblage theory outlines the actors involved, the theory of surveillance capitalism unleashes the purposes like profiling, targeted advertising, and marketing. The following chapters attempt to define the setting of an Indian school, which specific technological practices are underway and the impact of AI technologies, thus juxtaposing features of a panopticon, surveillant assemblage and surveillance capitalism in an Indian setting. The upcoming chapters will show in detail how children are identified and classified arbitrarily by deployed AI technologies, proving classroom to be a panopticon, surveillant assemblage and embodies the features of a control society.[106]

While each surveillance theory above has certain overlapping and distinct characteristics, it is important to note here that with each environment, context or setting, the nature of surveillance might differ. A particular scenario might have features squarely fitting into one or more of the theories described above. However, the impact of the surveillance by AI technologies remains common i.e., they hold power to endanger the informational and decisional privacy.

While we have looked at the advancement of the surveillance theories and how technology exacerbates the effects of monitoring, it is also essential to trace back the history, reasons, and motivations behind technology deployment in India. Revisiting the history will not only situate the present thesis within an Indian setting but also connect the above-mentioned surveillance theories with the context within which the continuous monitoring of children is taking place.

[105]Oscar H. Gandy Jr, The Panoptic Sort: A Political Economy of Personal Information, Critical Studies in Communication and in the Cultural Industries (Westview Press 1993).
[106] Infra, Chapter 4 and 5.

PART C: SCHOOLS AND PRIVACY

3.1. Genesis of Surveillance Schools

CCTV, Fingerprinting, facial recognition, palm vein scanners, etc., are a range of surveillance systems installed in schools.[107] Great Britain is reported to have installed CCTV cameras in 85-90 per cents of schools for student monitoring purposes.[108] Big Brother Watch released data on the level of use of CCTV in British schools in September 2012. Freedom of Information Requests (FOI) was sent to 4,092 secondary schools to ask for data about the number of cameras at the school premises. Among these 2,107 respondents, 90% have CCTV cameras. Big Brother Watch has reported that more than 100,000 CCTV cameras operate in High schools and academies in England, Scotland, and Wales. It should be noted that using CCTV cameras in schools is highly diverse. Some schools use a handful of strategic cameras in some areas, while others monitor nearly every field of vision with cameras, including classrooms, corridors, and sports facilities. Schools in various counties are familiar with hidden cameras that often directly link their devices to the police station.[109] Most often, CCTV cameras are equipped with audio recording technologies to assist visual imagery recorded by CCTV as well.

Similarly, India is witnessing the most common manifestation of school surveillance technologies in the form of visual surveillance techniques such as CCTV.[110] Post the Ryan School Murder case in the Gurgaon district of Haryana, CCTV cameras at schools in India's capital - New Delhi, increased.[111] Government officials have instilled a sense of fear and concern among the public that facilitates the installation of CCTV cameras to protect children from that same fear and provide a sense of protection. Nevertheless, it is generally accepted that these cameras are also

---

[107]. Roberts, J. Zhang, J. Truman, and T. D. Snyder, "*Indicators of School Crime and Safety: 2011*" (National Center for Education Statistics, US Department of Education, and Bureau of Justice Statistics, Office of Justice Programs, US Department of Justice, 2012), available at: http://nces.ed.gov/pubsearch/pubsinfo.asp.

[108] Big Brother Watch, "*Class of 1984: The Extent of CCTV in Secondary Schools and Academies*" (2012), London, available at: https://www.bigbrotherwatch.org.uk/files/school_cctv.pdf (consulted August 2016).

[109] Tyson Lewis, "The Surveillance Economy of Post-Columbine Schools" (2003) 25 Review of Education, Pedagogy, and Cultural Studies/JTL p. 335-355.

[110] Neha Miglani and Patricia Burch, "*Educational Technology in India: The Field and Teacher's Sensemaking*" (2019) 16 Contemporary Education Dialogue 26-53.

[111] Express Desk, "Ryan Murder Case: CCTVs, Verification of Staff among Rules CBSE has Issued for Schools" (Indian Express, September 14, 2017), available at: https://indianexpress.com/article/education/ryan-murder-case-cbse-issues-safety-guidelines-to-schools-gurugram/.

used to track the performance of students,[112] curbs general horseplay,[113] and 'eve-teasing', and to counter the mistreatment in the use of paper towels and soap in "toilets"- [114] apart from law enforcement purposes.

On the other hand, students across the globe have found ways to survive the glare of the camera. There are ways of resisting the gaze of CCTV -: students feel that it is necessary to avoid areas monitored by CCTV, to restrict CCTV's ability to recognise them and to reposition their activities cameras so they no longer control that activity.[115] However, despite resistance surveillance is increasingly being used as a tool to impart discipline and exercise power. These technologies are leading to children being more filtered with their lives being monitored and regulated in every aspect.

One of the prominent reasons that the Indian government uses to procure CCTV technologies or selling as an idea to parents/guardian of students, is the zero-tolerance approach towards bad behaviour, indiscipline, abuse among others.[116] An identical approach of zero-tolerance has been tried and tested in the UK, where CCTV cameras were first installed in schools for imparting a disciplinary approach. This innovative strategy of zero-tolerance with technology integration was introduced by then-Secretary of State Ruth Kelly in the UK in 2005, upon launch of which she stated:

> *"We must now have zero-tolerance of bad behaviour in the classroom and create a culture of respect, of good behaviour and firm discipline, and this must be the norm in all schools in every classroom all of the time."*[117]

---

[112]"CCTV Could Be Used in Exam Rooms" (BBC News, April 11, 2008), available at: http://news.bbc.co.uk/1/hi/education/7342432.stm.
[113] "Teachers Watched on CCTV Cameras" (BBC News, March 4, 2009), available at: https://www.bbc.co.uk/news/uk-scotland-tayside-central-21716049.
[114] "School Head Defends Toilets CCTV" (BBC News, January 27, 2009), available at: http://news.bbc.co.uk/1/hi/wales/mid/7851282.stm.
[115] Michael McCahill and Rachel Finn, "*The Social Impact of Surveillance in Three UK Schools: 'Angels', 'Devils' and 'Teen Mums*" (2010) 7 Surveillance and Society ¾. Emmeline Taylor, "*I Spy with My Little Eye: The Use of CCTV in Schools and the Impact on Privacy*" (2010) 58 The Sociological Review 3 381-405.
[116] Times of India, *Sexual Assault of a 3yr old at school*, Sep 01, 2023, Available at https://timesofindia.indiatimes.com/city/delhi/sexual-assault-of-3-yr-old-at-school-delhi-govt-tells-hc-it-has-zero-tolerance-towards-such-abuse/articleshow/103287711.cms?from=mdr.
[117]Paul Howard, Beyond Punishment: Reframing Behaviour in Schools (CfBT Education Trust 2009).

Further, the Education Secretary in 2011 stated:

> *"Our bill will put heads and teachers back in control, giving them a range of tough new powers to deal with bullies and the most disruptive pupils. Heads will be able to take a zero-tolerance approach."*[118]

Ruth Kelly was speaking of zero-tolerance of disruptive behaviour. But rather than creating a better and more secure school atmosphere through the expulsion of disruptive students, the zero-tolerance approach applied to schools via constant monitoring proved to be less effective in school conditions and under school management. [119] This is because a technology ignores the contextual setting, its subjectivities, and experiences while its operation. For instance, would the term 'indiscipline' indicate non-compliance with the laws of the school or opposition to them? Is it too uncertain and vague? Is a violent child termed 'potentially at risk'? Who will decide the grounds of bullying behaviour? These questions remain unaddressed in UK then and in India now and provide a starting point in this thesis for research in the Indian context.

There are now calls for a more measured approach that takes account of the nuanced nature of violations of rules, the extenuating circumstances, and the necessity of judgement and discretion rather than the zero-tolerance approach. For instance, in the United States, in Indiana, Texas, and Virginia, legislation has been introduced to change zero-tolerance policies or to expand schools' disciplinary options. Similarly, in England, some councils sought a ban on short-term suspension following excessive zero-tolerance use, which led to the inflationary suspension and expulsion rates.[120] Scholars favour a restorative justice approach that involves stakeholders and students in an interactive remedial process to deal with the cause of misconduct and damage. [121] However, the increased use of surveillance via CCTV and other emerging AI technologies can run counter to reliance on such nuanced approaches.

It is time for the legal system to take note of the intrinsic relationship between the right of children to make autonomous decisions, have more control over their personal information and the

---

[118] "'Teachers Able to Confiscate Mobile Phones to Control Disruptive Pupils'" (The Telegraph, July 3, 2010).
[119] American Psychological Association Zero Tolerance Task Force, "*Are Zero Tolerance Policies Effective in the Schools? An Evidentiary Review and Recommendations*" (2008) 63 The American Psychologist 9 852.
[120] Supra note 75.
[121] Belinda Hopkins, "*Restorative Justice in Schools*" (2002) 17 Support for Learning 3 144-149.

educational development of children in schools, who are under constant surveillance. In his book, '*The Country of First Boys*', Amartya Sen[122] reiterated this relationship:

> *"Development cannot be seen as increasing inanimate objects of convenience or promoting industrialisation or technological advance or social modernisation. These accomplishments are crucially important, but their value must depend on what they do with the lives and freedoms of the people involved. For human beings with responsibility for their choice, the focus must ultimately be on whether they have the freedom to do what they have reason to value. In this sense, the development consists of an expansion of people's freedom."*

The essential point that Sen tries to make here is that the legal system is the bedrock of providing both security and freedom to human beings, and the government should strive to create a condition where those fundamental rights can be realised. So, what is the fundamental right to privacy that we are seeking to protect? Is it related to intimacy, secrecy, limited access to oneself, liberty to make own decisions or control over your own information? Does surveillance further stretch the boundaries of conceptualisation right to privacy? Is it even possible to safeguard individual's right to privacy in a surveillant capitalistic world that is turning school into a panopticon or a surveillant assemblage?

PART D - THE DILEMMA OF LOCATING THE RIGHT TO PRIVACY IN THE SURVEILLANCE AGE

Jerry Kang, in *Cyberspace Terrorism,* has observed the threat of surveillance in the information age using the following words:[123]

> *"Data Mining in cyberspace produces detailed, computer-processable information, indexed to the individual, and permanent. Combine this with the fact that cyberspace makes data collection and analysis exponentially cheaper than in real space, and we have what Roger Clarke has identified as the genuine threat of dataveillance."*[124]

[122] Amartya Sen, The Country of First Boys and Other Essays (Oxford University Press 2015) 80-81.
[123] Jerry Kang, "*Information privacy in cyberspace transactions*" Stan. L. Rev. 50 (1997): 1193.
[124] Roger, Clarke, "*Information technology and dataveillance*" *Communications of the ACM* 31, no. 5 (1988): 498-512.

The data controller suppresses individuality by regular monitoring as characterised by 'Big Brother'. It studies the behavioural pattern of prospective data subjects and exploits them for their business interests. The dangers of surveillance have been exacerbated due to the aggregation of several databases and the opaque functioning of the autonomous systems, leading to self-censorship, obedience, and coerced conformity.

It is important to note here that the data controller does not coerce power; rather, the power is internalised into the minds of the society by social conditioning, manipulation, and indoctrination. Franz Kafka's 'The Trial' is the aptest metaphor to examine the discourse of a society under dataveillance. As Daniel Solove puts forward:

> *"The Trial captures the sense of helpfulness, frustration and vulnerability one experiences when a large bureaucratic organisation has control over a vast dossier of details about one's life".*[125]

A similar example of a state-orchestrated dataveillance in India is the introduction of a digital identity card called 'Aadhaar'. The government mandates Aadhaar's usage to avail the benefits of public services. Biometrics like iris scans, fingerprints and facial prints are collected and processed for Aadhaar to function. The said biometrics are stored in a centralised data processing system to which other databases (ranging from education, health, transportation, insurance, birth certificates, income tax returns etc.) are linked. Thus, Aadhaar not only enables the distribution of public services (for which it was initially introduced) but provides a 360-degree view of an individual based on which an individual is being quantified and categorised (further discussed in detail in Chapter fourth.[126]

But how did surveillance and identification through it become a norm? The "war on terror" was triggered by the attacks on the twin towers on 11th September 2001; the attacks and subsequent events have had a long-standing impact on the issue of security. The solution that was tempting in a climate of fear and concern was - in part – to rely on surveillance intended to harness data of everyone at a vast scale that increases the probability of finding the perpetrators and, in some cases, preventing an incident from occurring. Due to the emergence of sophisticated and

[125] Daniel Solove. "*Privacy and power: Computer databases and metaphors for information privacy*", Stan. L. Rev. 53 (2000): 1393.
[126] Refer to Infra Chapter 4, pg., 100-102.

integrated information collection technologies, surveillance became an intrinsic tool for counter-terrorism purposes. Furthermore, countries are updating or adding legislation to allow absolute power to surveil their citizens, often also applying such powers extraterritorially. Post-September 2001, privacy and security are pitted against each other because it may be perceived that only one can be protected in any given instance. Privacy often loses out to security because life and limb are at stake in the latter's case. As Professor Daniel Solove argues against this all-or-nothing proposition and argues that protecting privacy should not be understood as a tradeoff against security; instead, there should be call for greater transparency and accountability while deploying security measures.[127] For instance, facial recognition cameras are deployed in a classroom to impart security within the school premises. Questioning the deployment of such cameras to protect students' privacy does not speak against the security that each child should be afforded; rather it examines the regulation and oversight of the data collected by such cameras, shared by the school administration, and stored by the private entities. Thus, the debate between privacy and security is a flawed notion when both can be meaningfully evaluated together and balanced against each other on a basis of proportionality.

Privacy is an important constituent of human rights regarding definition and circumscription.[128] The right to privacy is considered one of the fundamental human rights in Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the ICCPR. For a long time, the concept of privacy as a specific right outside the public domain has traditionally taken on increasing forms of human contact and behaviour in different times and cultures.[129] A long and ongoing controversy has culminated in a search for a widely agreed description, which needs to be more robust and useful, as Chapter 3 will show in greater detail.[130] Nevertheless, the age of surveillance has made it more imperative that the word privacy be established, and it is necessary to set out reasonable areas where a claim of right to privacy is reasonably expected.

To effectively locate the right to privacy within the surveillance age, both the courts and the legislature need to rethink the powers granted to law enforcement agencies and regulatory authorities, especially in times of crisis, like national security, for the prevention of public order,

[127] Solove, Daniel J. "Nothing to Hide: The False Tradeoff Between Privacy and Security" (2012): 103-106.
[128] James Michael, *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology* (Dartmouth Pub Co 1994).
[129] Debbie VS Kasper, "The Evolution (or Devolution) of Privacy" (2005) 20(1) *Sociological Forum* 69.
[130] Raymond Wacks, *Personal Information: Privacy and the Law* (Clarendon Press 1993).

protection of sovereignty and integrity of the nation. Furthermore, historically, in "times of crisis", the state has been given absolute power to make rules and regulations through delegated legislation that does not come under the purview of parliamentary approval.[131] The courts also defer decision-making in such situations, leaving various government activities, including information-gathering, storing, sharing, and accessing, unregulated.[132]

The legislation should not strive to protect security at the cost of privacy; otherwise, it might risk being the cause of increasing privacy breaches. For instance, the Information Technology Guidelines for Cybercafe Rules, 2011,[133] require cyber cafe operators in India to maintain records of user identification (Aadhaar Card Number, PAN Card etc..) and user browsing information. In effect, these rules take away the ability of the user to browse anonymously as the information is retained, stored for one year. Such information must be shared with law enforcement agencies in case they require it for enforcement purposes. The said legislation is correct in asking to share private browsing information for law enforcement, national security purposes, or to prevent crime. However, it overlooks regulation and oversight as to how such data is shared, and stored, for how long it is to be retained, and thereby risks undermining the right to privacy. Since India lacks data retention policies, cybercafes have no transparency and accountability regarding their compliance with the sunset clause on data storage. Retaining data at multiple points, at cybercafes, with the Internet Service Provider and the application service provider acts as leakage points making personally identifiable information vulnerable. Indian cyber cafes, to seek compliance with ISPs and the government and to avoid disapproval of their licenses, regularly thwart the self-determination of their customers, an important facet of informational and decisional privacy.

Thus, the flawed privacy v. security debate permeates the country's executive, legislature, and judiciary which results in lesser protection of individuals privacy, especially in space like schools, where students' security or educational development takes precedence over privacy. In order to improve the debate between security and privacy, and to give equal importance to privacy, the

[131] Eichler, Jessika, and Sumit Sonkar. "Challenging absolute executive powers in times of corona: re-examining constitutional courts and the collective right to public contestation as instruments of institutional control." *Review of Economics and Political Science* 6, no. 1 (2021): 3-23.
[132] Khosla, Madhav, and Milan Vaishnav. "The three faces of the Indian state." *Journal of Democracy* 32, no. 1 (2021): 111-125. Also see, Gautam Bhatia, "The Troubling Legacy of Chief Justice Ranjan Gogoi," The Wire, 16 March 2019; Anup Surendranath et al., "Justice Arun Mishra and the Supreme Court's Rule of Whim," Article 14, 5 September 2020, www.article-14.com/post/justice-arunmishra-the-supreme-court-s-rule-of-whim.
[133] Department of Information Technology, Information Technology (Guidelines for Cyber Cafe) Rules, 2011, http://deity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf.

thesis needs to: a) *First*, layout the multiple forms that a right to privacy can take in regard to its conceptualisation, and b) *Second*, provide a framework that catalyses the examination of right to privacy in any given scenario.[134]

4.1. CONTEMPLATING THE NUANCES OF 'PRIVACY'.

In one of his judgements, Judge Richard Posner stated that privacy could mean withholding accurate information from the marketplace. Here he is viewing the right to privacy as typically concerning 'whether a person should have a right to conceal discreditable facts about himself'.[135] Thus, the right to privacy is viewed as a right of confidentiality or secrecy. Another example of a violation of privacy is a technology processing large quantities of personal data electronically. As a result of this, data collection and data processing conducted without consent does not violate confidentiality but the autonomy of an individual to share information with a limited set of people.[136] Depending upon the amount and type of data collected and processed, it can be used to sort, categorise, and profile individuals, leading to undervaluing the power and limiting the available choices for an individual. Thus, a right to privacy can also be conceptualised from a lens of power and control over a space or information. In his seminal paper, Conceptualising Privacy, Daniel Solove examines the claims made by academicians. It distils into six different nuances of privacy: the Right to be alone, Limited access to self, secrecy, intimacy, personhood, and informational privacy.[137] For instance, according to Arthur Miller, privacy is exasperatingly vague and evanescent.[138] As Hyman Gross says, pernicious ambiguities exist in the privacy principle.[139] Several authors have argued that privacy should be established in terms of 'intimacy'. According to Julie Inness, privacy content is captured when we focus exclusively on information, access, or private decisions because privacy can cover all three areas.[140] For example, affiliations and faiths may not necessarily be personal, but one might find them private. The definition of privacy by Samuel Warren and Louis Brandeis is also too general, as they define privacy as the right to be

[134] Infra, Chapter 3 provides a deep analysis of both the points.
[135] Posner, Richard A. *Economic analysis of law*. Wolters Kluwer law & business, 2014.
[136] Solove, Daniel J. "Privacy and power: Computer databases and metaphors for information privacy." *Stan. L. Rev.* 53 (2000): 1393.
[137] Solove, D.J., Conceptualizing privacy. *California law review*, pp.1087-1155, 200
[138] Ashman, Charles R. "The Assault on Privacy by Arthur R. Miller." *DePaul Law Review* 20, no. 4 (2015): 1062.
[139] Gross, Hyman. "The concept of privacy." *NYUL Rev.* 42 (1967): 34.
[140] Hixson, Richard F. "Privacy, Intimacy, and Isolation. By Julie C. Inness. New York: Oxford University Press, 1992. 157p. $24.95." *American Political Science Review* 87, no. 1 (1993): 202-202.

left alone.[141] Professor Solove concludes by stating that each context and practice will generate a form of indigestible privacy in another context.[142] Thus, rather than finding a common denominator of privacy, the endeavour should investigate a particular contextual setting and locate the essence of the right to privacy.

As a follow-up to the Conceptualising Privacy paper, Solove proposes a Taxonomy of Privacy in the context of the data mining conducted by the US government and law enforcement agencies.[143] The Taxonomy is divided into four key stages of data mining: information gathering, data processing, data sharing, and invasion. In 2006, Professor Solve identified the nuances of privacy at each data mining stage relevant to the current society's disruptions in the wake of the digital economy. The paper highlights the different harms and effects that can be caused to an individual's well-being because of data mining.[144] The present thesis takes a step further in *first* detailing the contextual setting (school) where the right to privacy is situated[145], *second,* bringing forth the nuances of privacy in the specific setting that overlap with the taxonomy provided by Professor Solove[146], and *lastly*, providing a regulatory framework for courts and policymakers that recognises the socio-technical landscape within which a right to privacy sits.[147]

4.2. INFORMATIONAL AND DECISIONAL PRIVACY: THE TWO COMPLEMENTING RIGHTS

In the information revolution age, from our credit card information, our watching patterns on television, our entry and exit from a public/private place to our heart rate, mobility patterns and dietary habits, rivulets of information flow into robust algorithmic systems. Both over-the-skin and under-the-skin surveillance is rampantly deployed across the globe.[148] It is possible to build an electronic collage of an individual's location, purchases, hobbies, likes and dislikes through computer networks' complex and chaotic world. This amassing of information creates a breach of informational privacy - *'collection, use and disclosure of personal information*'. It is because of

[141] Brandeis, Louis, and Samuel Warren. "The right to privacy." *Harvard law review* 4, no. 5 (1890): 193-220.
[142] Supra 125, pg., 1091-1093.
[143] Solove, D. J. (2005). A taxonomy of privacy. *U. Pa. l. Rev.*, *154*, 477.
[144] Ibid, pg., 470.
[145] Infra Chapter 4.
[146] Infra Chapter 5.
[147] Infra Chapter 6.
[148] Harari Y.N., The world after coronavirus, Financial Times, Mar 20, 2020. Available at https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75.

data collection and processing that gives the data controller the power to interfere with the intimate decisions of an individual.

As Helen Nissenbaum states,[149]

> *"It is not conceptual but casual for privacy is claimed to be an important aspect of an environment in which autonomy is likely to flourish, and its absence likely to undermine it."*

The act of deception or coercion, leading the individual to make decisions, choices, or take actions, violates decisional privacy, or as Dworkin says,[150] '*makes an individual an instrument of another's will'*. The incessant collection and processing of data also create a breach of decisional privacy. At its core, decisional privacy is the right not to be interfered with in making core life decisions regarding who we are, how we define ourselves and how we want to behave. Broadly, in India, the judiciary has interpreted the right through the lens of individual liberty - the right to take abortion decisions,[151] food choices,[152] the right to love[153] etc. Globally, decisional privacy has remained one of the most heated and socially divisive issues, like in cases involving abortion and euthanasia. The courts worldwide have treated decisional privacy to provide liberty, autonomy, or personhood in making life decisions. However, when it comes to children, the presumption that parents act in the best interests of their children precludes a child from making decisions on their behalf. Children lack the judgement, maturity, and experience to make life-altering decisions. Thereby minors' interest in concealing their sexual life, the choice to get aborted or the freedom to use their data in the manner they want is not constitutionally protected unless parents/guardian is involved. This is where informational privacy (control over data collection or sharing) and decisional privacy (liberty to make decisions with autonomy and dignity) overlap and complement each other. The thesis outlines' mechanisms for the effective involvement of children in decisions regarding the design, development, and deployment of technologies as they are the ones directly affected at each stage of the AI technologies lifecycle. Such active participation/involvement provides them effective rights in a data protection legislation, means to seek grievance redressal,

[149] Nissenbaum, Helen. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, 2009, p. 82.
[150] Dworkin, Gerald. *The theory and practice of autonomy*. Cambridge University Press, 1988.
[151] *Suresh Kumar Koushal v. Naz Foundation*, (2014) 1 SCC 1. See also Justice Balakrishnan's opinion in *Suchita Srivastava v. Chandigarh Administration*, (2009) 9 SCC 1.
[152] *Haresh M. Jagtiani v. The State of Maharashtra*, Writ Petition No. 982 of 2015, Bombay High Court.
[153] *Navtej Johar v. Union of India* AIR 2018 SC 4321.

power, and control over their personal information, all contributing to safeguarding their right to privacy.

CONCLUSION

This chapter sets out the background to the whole thesis, by first laying out the socio-technical conceptualisation of technology in Part A, as illustrated by Michel Foucault. Herein, technology is evaluated not as a mere machine, but as an embodiment of societal practices. Such conceptualisation ties nicely with Bentham's different architectures of the Panopticon and Foucault's panopticism, as outlined in Part B of this chapter. Inherently, the panopticon is not a technology but an architecture in which the subjects are disciplined by means of a continuous gaze. An omnipresent power by keeping a gaze across the architecture produces docile bodies. With the emergence of surveillance technologies, architecture has seen a shift whereby everyone is under surveillance in a nation-state, unlike in a panopticon, where only individuals inside a particular architecture are monitored. This second stage of surveillance has been made possible due to the emergence of private actors, and capitalist forces with neoliberal ideas. Their aim is not to discipline the subjects but instead to create a controlled society and yield profit. The most recent, i.e., the third stage which is further branched out (like a rhizome), has seen an amalgam of public-private partnerships, the state and the market coming together and engaging in acts of surveillance. The third stage is where the state absolves itself of all its duties and provides power to the market to design, develop and deploy surveillant infrastructures. Part C of the chapter provides a glimpse of how the third stage has reached Indian schools, trampling upon students' right to privacy. But Part D raises the dilemma of privacy v. security in which the latter is given preference over the former. It might be due to the different nuances of the right itself that creates a barrier in terms of its effective operationalisation. Right to privacy takes multiple forms of intimacy, secrecy, right to be let alone, limited knowledge to oneself among others, depending on the contextual setting. While in cases involving CCTV cameras, the question is of collection of data without consent, in scenarios involving facial recognition or other AI technologies, the question is of prediction and presumption. Academicians, including *Kenneth Karst* warn about making choices about an individual based on selective knowledge. Karst notes, '*facts stored about an individual will become the only significant facts about the subject of the inquiry*', infringing informational and decisional privacy.[154] It raises the question of whether privacy is a contextual

[154] Kenneth L Karst, "*The Files: Legal Controls over the Accuracy and Accessibility of Stored Personal Data*" (1966) 31(2) Law and Contemporary Problems 342.

right and is thereby difficult to conceptualise? If it cannot be conceptualised how can the risks of AI technologies, making schools a panopticon or a surveillant assemblage, be understood, evaluated, and mitigated?

The next chapter begins examining the right to privacy in a hope to come up with a framework that enables the understanding of the said right. Then the subsequent chapters evaluate the novel challenges of the AI technologies and the context-dependent privacy risks that they emanate before the final chapter proposed mitigating steps.

THIRD CHAPTER

UNDERSTANDING THE RIGHT TO PRIVACY

In one of Professor HLA Hart's observations, he notes, "*In law as elsewhere, we can know and yet not understand*".[155] The statement suits the word 'privacy' as there have been various conceptualisations, a synoptic view of which the present chapter provides. Nevertheless, the uncertainty around the word's meaning makes applying a legal framework and seeking protection challenging. We will see in this chapter how, due to the variable meaning of privacy, we have put ourselves in a position where we are unable to comprehend it, as it is a contextual right. This chapter presents a partly abstract discussion of the 'right', but in Part B of this chapter the Indian jurisprudence on privacy, reflecting the position in the Indian Constitution is considered, relating it to the background context in the previous chapter.[156]

In **Part-A**, this chapter provides potential conceptions of privacy by recognising and critiquing its established explications in legal theory. Part-A uses Daniel Solove's study of privacy to dissect the theoretical constructs of the right. Solove's each deduced conceptualisation is then located within Indian legal jurisprudence to show how courts have conceptualised Privacy, sometimes even diluting and misunderstanding or confusing its meaning, thus contributing to its imprecision. The need to discuss the right to privacy is due to different forms and shapes it takes depending on a context. This part also demonstrates that while a right to privacy is dependent on a context, it has certain core constituents that remain the same across geographies and cultures. Further, the chapter discusses Informational Privacy separately in **Part B**, as it forms the core of the present thesis around which a legislative framework is drawn. Though Part-A highlights the complexities in coming up with a common definition of Privacy, Part B dives in-depth into informational and decisional privacy undergoing shifts with each technological development, making it an amorphous concept. Part B also evaluates the Indian jurisprudence on this 'right'.

Part C questions the earlier two parts by asking whether it is even possible to conceptualise Privacy in the sense of not making it over-inclusive or under-inclusive. Daniel Solove also points out that there is no common denominator of Privacy but "*a cluster of many distinct yet related*

[155] Hart, Definition and Theory in Jurisprudence 3 (1953), pp. 34-35.
[156] Infra Part B, pg. 64-80.

things".[157] The chapter, taking note of Helen Nissenbaum's pioneering work, affirms that each context has many people, communities, and institutions involved that shape privacy as a concept, making it a highly contextualised issue. It concludes that conceptualising privacy to reach a single theory is useless and will only add to the chaos and uncertainty of earlier work. However, it recognises the effort taken by academics to come up with certain core constituents of the right to privacy. The chapter concludes by advocating for outlining the structures, processes, and people involved in a context (in the thesis's sense, the education sector) to examine the nature and scope of invasions of the right to privacy, rather than conceptualising it.

PART A - CONCEPTUALISING PRIVACY

Judith Jarvis Thomson begins her article with, "*Perhaps the most striking thing about the right to privacy is that nobody seems to have any clear idea of what it is*".[158] After almost 50 years, her observation still holds, but with a new sense of urgency - mainly due to the advancement of technology.

1.1. Right to be Let alone

Multiple scholars recognise the first conceptualisation of privacy as the '*Right to be let alone*' propounded by Samuel Warren and Louis Brandeis.[159] However, some, like Hyman Gross, also consider such a conceptualisation as approaching retirement because it describes privacy rather than offering a definition.[160] Warren and Brandeis' underlying principle in law protects the individual from unlawful interference in person and property. Such a conception originates from common law, which remedies physical interference in body and property, as in the tort of battery in its various forms and trespass. Gradually, such legal rights broadened to encompass the protection of a person's mental well-being, like the Right to enjoyment of personal life without

[157] Solove, D. J. (2008). Understanding privacy, p. 40.
[158] Thomson, J. J. (1975). The right to privacy. *Philosophy & Public Affairs*, 295-314.
[159] Brandeis, L., & Warren, S. (1890). The right to privacy. *Harvard law review*, *4*(5), 193-220. Though the credit for giving privacy's first definition goes to Samuel Warren and Louis Brandeis, they were careful of giving this credit to Justice Thomas Cooley. Justice Cooley recognised that the right to personal security is an absolute right vested by the immutable laws of nature. It means that a person should enjoy uninterrupted enjoyment of his life, limbs, body, health and reputation. It is this right that Justice Cooley recognises as the 'right to be let alone', later adopted by Warren and Brandeis. For greater detail, read Cooley, T. M. (1906). *A Treatise on the Law of Torts, Or the Wrongs which Arise Independently of Contract* (Vol. 2). Callaghan. For authors who hail Warren & Brandeis's formulation, see Kramer, I. R. (1989). The Birth of Privacy Law: A Century Since Warren and Brandeis. *Cath. UL Rev.*, *39*, 703, Kalven Jr, H. (1966). Privacy in tort law--were Warren and Brandeis wrong. *Law & Contemp. Probs. 31*, 326., Gavison, R. (1980). Privacy and the Limits of Law. The Yale law journal, 89(3), 421-471.
[160] Gross, H. (1967). The concept of privacy. *NYUL Rev.*, *42*, 34.

intrusion (respect for private life in Article 8 ECHR), which includes the Right to be let alone. The regard for emotions or sensations meant that the protection went beyond the individual's body like the tort of nuisance. The said tort was developed with protection against odours, smoke, noises, and excessive vibration. Similar development within the Right to enjoyment of life was seen in the conception of the Right to property, encompassing both corporeal and incorporeal rights. Warren and Brandeis make it clear in their seminal piece the extent of such protection depends on political, social, and economic changes in society,[161] making the conception of Privacy a fluid and contextual issue. For instance, their piece talks about how persistent circulation of personal gossip in the form of news can pollute the thoughts *and aspirations of the people*. Continuous feeding of immoral, unethical, or simply lame news can potentially destroy one's consciousness and '*robustness of thought*'.[162] Such a form of news belittles other notions of relative importance that a human brain could have thought of or processed as students at Harvard Law School. Warren and Brandeis were witnesses of rapid urbanisation and its technological advances in Boston. Window glasses, photography, and the telephone invention in Boston were technologies that saw a rise in its consumers due to their inexpensiveness. However, such technologies coupled with '*newspaperisation*'[163] also increased the vulnerability of individuals (unknown at that time) as their actions, images and personality were exposed to a broader set of people. Thus, more significant intrusion into the private lives of individuals became rampant.

In India, the courts have also dealt with a challenge regarding interference with an individual's body and mental processes. The judgement in *Selv*i v. *State of Karnataka*[164] balanced the Right to non-self-incrimination and privacy. In this case, three interrogation techniques, namely, narco-analysis, polygraph, and Brain Electrical Activation Profile, were used on the Appellants. The appellants argued against banning them because they interfered with the individual's autonomy and the right to be alone. The Chief Justice stated:

> "*We must recognise the importance of personal autonomy in aspects such as the right to speak or to remain silent. Further, forcible interference with a person's space or body,*

[161] Id., 193.
[162] Id., 196.
[163] The word '*Newspaperisation*' was coined by Henry James in response to describe the context which Samuel Warren and Louis Brandeis use to design their theory around Right to Privacy. For detail, see James, H. (1922). *The Reverberator: Madame de Mauves; A Passionate Pilgrim; and Other Tales* (Vol. 13). C. Scribner's Sons.
[164] (2010) 7 SCC 263.

> *which includes mental processes, goes against its inviolable personality, thus violating the prescribed boundaries of privacy."*[165]

The Court in *Selvi* conceptualised Privacy as a core element of personal liberty, autonomy and dignity, core to the existence of a human being. Using such interrogation techniques on an individual's body removes its Right to determine to what extent its thoughts, sentiments, and emotions shall be communicated to others. It would amount to a violation of a right and go against the Constitution's preamble.[166] Thus, any physical or mental intrusion with an individual violates their Right to freedom to believe in what is right and thus impairs the Right to be let alone. Justice Mathew, in his minority opinion in the landmark case of *Kesavananda Bharati v. State of Kerala*, observed:

> "*The social nature of man, the generic traits of his physical and mental constitution, his sentiments of justice and the morals within, his instinct for individual and collective perspectives, his desire for happiness, his sense of dignity, his consciousness of man's station and purpose in life, all these are not products of fancy but objective factors in the realm of existence.*"[167]

Privacy and liberty are inseparable; the former is a precondition to enjoying the latter.[168] Justice Matthew's thoughts in *Kesavananda* resonated with what the U.S. Supreme Court recognised in *Roe v. Wade* in the same year.[169] By taking note of Justice Brandeis's opinion in *Olmstead v. United States*[170], S.C. stated that the government must ensure conditions favourable to the pursuit of happiness. The U.S. S.C. meant that a sphere should be conferred upon an individual against

---

[165] Ibid, p. 369-370, pp. 225-226.

[166] The Preamble of the Indian constitution postulates Liberty of 'thought, expression, belief, faith and worship'. It is considered the basic structure of our constitution as propounded in Kesavananda Bharati Case (Infra, note 10), which should be adhered to in all cases. The fundamental rights embodied in the Indian constitution are considered a necessary consequence of the declaration in the preamble. The position has been clarified by the constitution bench of the supreme court in *Behram Khurshed Pesikaka* v. *The State of Bombay*, (1955) 1 SCR 613.

[167] *Kesavananda Bharati* v. *State of Kerala*, (1973) 4 SCC 225, pp. 1676.

[168] Laurence H. Tribe and Michael C. Dorf, Levels of Generality In The Definition Of Rights, 57 U. CHI. L. REV. 1057 (1990) at 1068.

[169] 410 U.S. 113 (1973).

[170] 277 US 438 (1928). Delivered by Warren Brandeis himself who wrote the seminal article on Right to be let alone, explaining that during his time the common law of torts was incapable of providing redress to the injury to feelings. Such injuries invade an individual's life to plan his own affairs.

the government, where he should be left alone.[171] Though John Stuart Mill, in his seminal '*On Liberty*', did not use the terms 'privacy' or the Right to be left alone, but characterised liberty in a way that locates privacy as a necessary aspect of liberty. He appropriates liberty as consciousness and demanded liberty for the same, like freedom of thought, feeling, and opinion.[172]

1.2. Limited Access to Self

While the Right to be left alone can be characterised as an individual claiming solitude, the conceptualisation of Privacy as limited access to self-views solitude as just one of its components. For instance, minimal interference by the Government in an individual's life involves a right to remain alone. However, it also provides the individual with a sense of autonomy and control to decide the extent to which it wants to keep affairs public, i.e., protection from unwarranted access.[173] Thus, in this sense, the Right to Privacy allows one to choose a realm or community necessary to fulfil enjoyment in life. One of the profound proponents of this conceptualisation is Hyman Gross, who viewed Privacy as a condition of human life in which acquaintance with personal life is limited.[174] However, he explains this through the landmark decision of *Griswold v. Connecticut.*[175] In the decision of *Griswold v. Connecticut* it was found that each form of interference should not be comprehended as a violation of Privacy just for the sake of removing the ambiguity. In the case, the Connecticut Comstock Act of 1873 was constitutionally challenged by *Griswold* and Dr Buxton because a ban on contraception can threaten the lives and well-being of patients. In its majority opinion, the U.S. Supreme Court opined that the Bill of Rights specifies "*penumbras,"* i.e., zones of Privacy, among which one is the sacred '*association*' of marriage. Instead of proving the origin of marital Privacy from the Bill of Rights, the Court stated that the Right to Privacy is implied by specific provisions, for instance, the first amendment. Such discretion of the judges, in this case, is what Hyman argues against by showing the negative correlation between the provisions and the Right to Privacy. For instance, the first amendment talks about freedom of association and its linkage with freedom of speech and expression, wherein the provision grants specific associations like labour unions the right to express their opinions. Herein, the Court is arbitrary in its linguistic interpretation of the word '*association*' by including the sacred precincts of the marital bedroom within its ambit. The Court states, "*Marriage*

[171] Supra note 134, pp. 20.
[172] John Stuart Mill, On Liberty and other Essays 15-16 (Stefan Collini ed., 1989) (1859).
[173] Bok, S. (1989). *Secrets: On the ethics of concealment and revelation*. Vintage.
[174] Gross, H. (1967). The concept of privacy. *NYUL Rev.*, *42*, 34.
[175] *Griswold v. Connecticut*, 381 US 479 (1965).

is an association that promotes a way of life, not causes, a harmony in living, a bilateral loyalty and an association for as noble a purpose as any involved in our prior decisions'.[176]

If the article by Warren and Brandeis is read carefully, they move beyond simply supporting the Right to be let alone. They also discuss Privacy as an individual's desire to limit or broaden their body or property access.[177] Everyone has control over their thoughts, sentiments, and expressions, which they can use to limit or publicise personal information.[178] Such protection also has a basis in Intellectual Property Law, where novel expressions are accorded legal protection for monetary purposes. Herein, they argue that copyright statute aims to protect the author's profit from such expressions, which falls short of protecting the Act of the publication itself. Such protection is materialistic rather than spiritual as it protects any reproduction of the expressions - a corporeal property once published.[179] However, Warren and Brandeis talk about protecting incorporeal interests, like the effect of the publication on an individual. For instance, a letter written by the mother to her son is not of any value in the legal sense of 'property', though if reproduced, it has a bearing on mental peace due to its private contents. What about a 'gossipmonger' who publishes the letter's contents intended to be private? In the case of *Prince Albert v. Strange*, Lord Cottenham answered this query where an individual made unauthorised copies of etchings made by Queen Victoria and her husband for private enjoyment. Lord Cottenham accepted that "*a man is entitled to be protected in the exclusive use and enjoyment of that which is exclusively his*" and recognised that "*in this case, privacy is the right invaded*".[180] The said judgement indicates that an individual shows trust and confidence to a limited set of people, which, if broken, violates the Right to Privacy. Much earlier than Lord Cottenham's recognition of the word 'privacy', in another judgement, *Abernethy v. Hutchinson,*[181] Lord Eldon restrained the publication of unpublished lectures in Lancet magazine because of a breach of confidence. Lord Eldon held that if an individual is admitted as a pupil or otherwise, she has the authority to put down the lecture in shorthand but only publish it with the lecturer's consent. One can infer from Lord Eldon's

[176] Ibid, at 485-46.
[177] Supra note 141, Warren & Brandeis p. 199-205.
[178] Warren and Brandeis refer to Justice Yates' judgement in *Millar v. Taylor*. Yates, J. in *Millar v. Taylor*, 4 Burr, 2303, 2379 (1769).
[179] The main characteristics of a corporeal property that it is transferable, have a value, and can be either used or reproduced to realise the value.
[180] *Prince Albert v. Strange*, (1849) 47 ER 1302.
[181] 3 L.L. Ch. 209 (1825). Similar observations were made in *Tuck v. Priester*, 19 Q.B.D. 639 (1887) where the defendant was not allowed to sell copies of a picture owing to breach of confidence. Another notable judgement is *Pollard v. Photographic Co.*, 40 Ch. Div. 345 (1888) wherein the defendant was restrained from exhibiting a lady's photograph as it was not consented to be sold.

judgement that the lecturer must share his/her knowledge with the broader community. Thus, the lecturer's oral statements are meant for limited individuals, not considered their property. The power of judicial decision-making over the decades has aided in the growth and development of the Right to Privacy as a legal injury from the closet of tort law and law of literary and artistic property.

In India, Justice SA Bobde, in the landmark case of *K.S. Puttaswamy v. Union of India,* also conceptualised Privacy and limited access to self. He stated, "*One of the ways of determining what a core constitutional idea is, is to consider the opposite*". Just like freedom is the absence of restraint, Privacy is the absence of unwanted publicity. He correlates the concept of trust with Privacy using the earlier articulation of trust by the Supreme Court in *Deoki Nandan v. Murlidhar*.[182] The judgement laid out the difference between private and public trust, in which the former provides access to '*limited*' or specific individuals, and the latter is open to the public. Similarly, the Right to Privacy is a relational right wherein an individual 'chooses' and 'specifies' to include and exclude people.[183]

1.3. Secrecy

One of the common attributes of a privacy claim is disclosing concealed information, i.e., breach of secrecy. Secrecy is a way to keep private information to oneself wherein it breaches the territories of other conceptualisations of Privacy, i.e., limited access to self. In Indian jurisprudence, secrecy has often been propounded in fiduciary relationships,[184] like that of doctor-patient or lawyer-client, wherein a "duty of care" applies. Such is the landmark case of *Mr. X v. Hospital Z*,[185] in which the appellant doctor's blood sample was found to be HIV+. Upon disclosing this information by the respondent hospital, the appellant's marriage became broken, and she was forced to leave the State of Nagaland and settle in another part of India. The lower court judges fell back on the duty of care principle wherein the doctor must keep the patient's information secret. The Supreme Court went beyond the tort principle to hold that even public disclosure of facts violates the Right to Privacy as it breaches the confidentiality obligation. While laying out the importance of secrecy in an individual's life, the Court held that:

---

[182] (1956) SCR 756.
[183] Justice SA Bobde in his judgement referred to the act of choosing and specifying as autonomy in the negative. *K.S. Puttaswamy* pg. 37, pp. 43.
[184] For such purposes, refer to 8(1)(e) of the Right to Information Act which provides an exemption from furnishing information if the information was available to a person as part of a fiduciary relationship.
[185] (1998) 8 SCC 296.

> "*Disclosure of facts may generate many complexes in an individual's life, can disturb a person's tranquility and may even lead to psychological problems. The individual might have to lead a disturbed life all through. Considering these potentialities, the right to privacy is essential to the right to life under Article 21*".[186]

However, the Court also crafted that in cases where breaching confidentiality or secrecy contributes to a societal benefit or is in the public interest, it does not amount to a breach of Privacy. For instance, disclosing information in the hospital case saved the woman from getting infected; therefore, the doctor could not claim compensation. The reverse of this, where disclosure affects the confidentiality of the information, is also prohibited in India through the Official Secrets Act, 1923.[187]

Protection of secrecy of an individual or group has led to several court judgements often balancing constitutional rights against the Right to Privacy. One instance concern balancing the Right to information on the one hand and the Right to Privacy, both rights emanating from the Constitution of India. In the case of *Bihar Public Service Commission v. Saiyed Hussain Abbas Rizwi*,[188] the defendant sought information regarding judicial appointments made by the appellant, such as names, designation, addresses of experts on the interview board, names of candidates who appeared, criteria for selection and other details. Justice Swatanter Kumar, speaking for the Court, held that:

> "*Matters, particularly concerning appointments, are required to be dealt with great confidentiality. Secrecy of such information shall be maintained, thus bringing it within the ambit of fiduciary capacity.*"[189]

Secrecy is also talked about in the context of intrusions in the name of surveillance. In *Roman Zakharov v. Russia,*[190] The ECtHR examined the violation of Article 8 of the Convention as mobile operators allowed security services an unrestricted interception of all telephone communications

[186] Ibid, p. 307, pp. 28.
[187] The Official Secrets Act balances the need to be transparent to the public about government activities and the protection of sensitive personal information.
[188] (2012) 13 SCC 61.
[189] Ibid, p.74, pp. 23.
[190] European Court of Human Rights, Application number 47143/06.

without prior judicial authorisation. The Court held that surveillance measures are often secret and, in this case, lacked effective means to challenge them at the national level, amounting to interference by the State with the Right to Privacy of an individual. The Supreme Court of India expressed a similar view in *Kharak Singh v. State of Uttar Pradesh*,[191] where Regulation 237 of the U.P. Police Regulations, which granted surveillance powers to the Police, was challenged as violative of fundamental rights.[192] Justice Subba Rao and Justice Shah struck down the entire regulation as violating the Right to Privacy of an individual. Specifically commenting on Regulation 237(a), i.e., Secret Picketing of the house or approaches to the house, the Court stated:

> "*By shadowing every activity of the suspect, the individual's life was made an open book, and every activity of his was closely observed and followed. …. These are parts of surveillance which restrict the movements, encroaching an individual's private life.*" Violating the secret affairs of an individual to whom they meet or talk to is an integral part of an individual's domestic life, where "*it is expected to give him rest, physical happiness, peace of mind and security.*"[193]

Secrecy is a form of 'relational privacy' where an individual or a group of individuals exercise control over the flow of information. Selective disclosure is done voluntarily to limit the knowledge of oneself in society. George Simmel states that limiting knowledge about oneself is to exercise control over personal information or create a metaphorical space to self-realise.[194] Surveillance is the antithesis of self-realisation, limiting control over secrecy. The constant, pervasive intrusiveness controls an individual's imagination and emotions, which Noam Chomsky considers

---

[191] (1964) 1 SCR 332.

[192] The regulation stated: - "Without prejudice to the right of Superintendents of Police to put into practice any legal measures, such as shadowing in cities, by which they find they can keep in touch with suspects in particular localities or special circumstances, surveillance may for most practical purposes be defined as consisting of one or more of the following measures: -
(a) '***Secret'*** picketing of the house or approaches to the house of suspects.
(b) domiciliary visits at night.
(c) through periodical inquiries by officers not below the rank of Sub-Inspector into repute, habits, associations, income, expenses and occupation.
(d) the reporting by constables and chowkidars of movements and absences from home.
(e) the verification of movements and absences by means of inquiry slips.
(f) the collection and record on a history-sheet of all information bearing on conduct."

[193] Supra note 37, p. 358-359. These observations were taken by Justice Subba and Justice Shah from Justice Frankfurter in *Wolf v. Colorado* (1949) 338 U.S. 25 while talking about privacy from arbitrary intrusion by the police.

[194] Simmel, G. (1906). The sociology of secrecy and of secret societies. *American Journal of sociology*, *11*(4), 441-498.

absolute and essential to human development in its richest diversity.[195] Philosopher Thomas Nagel explains concealment as a condition of civilisation in the following words:

> "*Concealment includes not only secrecy and deception but also reticence and non-acknowledgement. Apart from everything else, there is inner life's sheer chaotic, tropical luxuriance. We also must learn not to be overwhelmed by the consciousness of other people's awareness of and reaction to ourselves - so that our inner lives can be carried on under the protection of an exposed public self over which we have enough control to be able to identify with it, at least in part.*"[196]

Thus, managing secrecy is about managing relationships between self and others. Alternatively, sociologist Nippert-Eng emphasises a "*boundary regulatory process*" that makes a person accessible.[197]

1.4. Personhood

According to Edward Bloustein, the term '*personhood*' relates to a person's individuality which the Right to Privacy seeks to protect.[198] This conceptualisation by Bloustein was in response to Dean Prosser's explanation of 'the invasion of Privacy as four distinct torts,[199] each containing an element of Privacy with distinct characteristics. The four identified areas of tort law were Intrusion, Public Disclosure, False Light, and Name Appropriation. In an attempt to conceptualise Privacy, Bloustein merges the torts mentioned above and claims that all of them embed a single claim of Privacy, i.e., violation of human dignity. Bloustein refers to intrusion as "*an affront to human dignity"* as it fails to respect individuals having free minds and souls, which should not be an object of someone's scrutiny. It is like the case of *Stanley v. Georgia*,[200] in which the Court upheld the Right to possess obscene material within the confines of one's private home. The Court stated that such a right is necessary to protect the first amendment for an individual's "right to satisfy its intellectual and emotional needs in the privacy of its own home".[201] Concerning *public disclosure*, invasion of Privacy is founded upon degrading an individual's reputation, honour, and dignity. In

[195] Chomsky, N. (2015). *What kind of creatures are we?* Columbia University Press, p. 60.
[196] Nagel, T. (2004). *Concealment and exposure: and other essays*. Oxford University Press, at p.4.
[197] Nippert-Eng, C. E. (2010). *Islands of privacy*. University of Chicago Press, p. 22.
[198] Bloustein, E. J. (1964). Privacy as an aspect of human dignity: An answer to Dean Prosser. *NYUL rev.*, *39*, 962.
[199] Prosser, Privacy, 48 Calif. L. Rev. 383 (1960).
[200] *Stanley v. Georgia*, 394 U.S. 557 (1969).
[201] Ibid, at 565.

scenarios involving *the appropriation* of an individual, the human decides the worth of the body - anything lower than which shall be considered exploitative. In such an attempt, rather than conceptualising Privacy, Bloustein constitutes another lexicon or referent object for Privacy, like autonomy. Such conceptualisation has been seen among various judgements in the Supreme Court of India, even before 2017, i.e., before the Right to Privacy was explicitly declared as a fundamental right.[202] In the case of *Prem Shankar Shukla v. Delhi Administration,*[203] *The Supreme Court of India,* while opining on the handcuffing of the prisoners, held that to "manacle an individual is more than to mortify and dehumanise its personhood violating the guarantee of its human dignity".[204] Such an act is more of a violation according to the Indian Constitution as the founding fathers of the document inserted Justice, equality and 'dignity' of the individual in its preamble, which reflects the core values of the Constitution. For autonomy, the *National Legal Services Authority v. Union of India* (NALSA)[205] is considered a landmark judgement that deals with the rights of transgender persons. The Court in *NALSA*, while indicating the protection of gender identity as an expression of personal autonomy, relied on the case of *Anuj Garg v. Hotel Association of India,*[206] in which the Court described personal autonomy as including both the negative Right of not to be subject to interference by others and the positive Right of individuals to make decisions about their lives, to express themselves and choose which activities to take part in. Self-determination of gender is an integral part of personal autonomy and self-expression and falls within Article 21 of the Constitution of India.[207] The court in NALSA also reiterated the "*golden triangle*" test,[208] which every case law needs to pass. He said that the test triangulates

[202] Infra, 267, *K.S. Puttaswamy v. Union of India*.
[203] (1980) 3 SCC 526.
[204] Ibid, p. 529-530, pp. 1.
[205] (2014) 5 SCC 438.
[206] (2008) 3 SCC 1, pp. 34-35.
[207] Supra note 39, at page 490, pp. 72.
[208] The golden triangle test comes in the case of *Maneka Gandhi v. Union of India* (1978) 1 SCC 248. This case is important to note in the development of fundamental rights jurisprudence. Pre-*Maneka Gandhi*, Article 21 was read literally, and each fundamental right was interpreted distinctively. However, *R.C. Cooper v. Union of India* [(1970) 2 SCC 298] partially, and then *Maneka Gandhi v. Union of India* fully overturned the water-tight compartment formula enunciated in *A.K. Gopalan v. State of Madras* AIR 1950 SC 27. The Court established the constitutional doctrine in these cases that Article 21 covers a variety of rights under the ambit of life and personal liberty, which all contribute to the autonomy and dignity of an individual, such as the right to privacy. Some rights recognised under Article 21 have been elevated to fundamental rights like freedom of speech and expression under Article 19. Hence Article 21 is a residue of other rights mentioned under Part III of the Indian constitution and overlaps with them. Now, for the justification of Article 19 and Article 21 being connected to Article 14 and forming a golden triangle, the court justifies that while protecting the rights, the court has to lay down a procedure which is just, fair and equal, i.e., non-arbitrary and non-discriminatory which is Article 14/15 of the Indian constitution. Thus, the decision in *Maneka*, while laying down the jurisprudential foundation of fundamental rights, also clarified that various deprivations could be classified as violations of right to privacy under article 21.

Article 14/15 (Right to Equality before the law and prevention of discrimination on specific grounds), Article 19 (freedom of speech and expression) and Article 21 (Right to life and liberty) of the Indian Constitution, which aids location of a constitutional right to Privacy as an expression of individual autonomy and human dignity.

In US legal jurisprudence, *Roe* [209] is one landmark judgement that enunciates Privacy as a concept of liberty and autonomy. In *Roe*, a Texas statute was in contention, which made abortion illegal, except in cases where the mother's life was in danger. The U.S. Supreme Court, by seven to two votes, declared the said statute to be unconstitutional. The Court here distinguished Griswold's opinion that Privacy is not necessarily inherent in marital Privacy. It reiterated the Court's judgement in *Eisenstadt v. Baird*[210] that Privacy is also the Right of an individual, whether married or single, to be free from governmental intrusion. It is upon the woman's liberty to make crucial decisions regarding her life, and herein, her body is integral to the sphere of her autonomy, which in *Roe* is also referred to as '*decisional privacy*'. However, the dissenting opinion of *Roe* did not object to the autonomy aspect of the judgement but countered the nature and source of Privacy as a constitutional right. In his dissenting opinion in Roe, Justice Rehnquist stated: The Court's opinion is far more appropriate to a legislative judgement than *a judicial one. The decision here partakes more of judicial legislation than it does of a determination of the intent of the drafters of the Fourteenth Amendment.*[211]

Justice Rehnquist's dissenting opinion has its inspiration from Justice Black's dissenting opinion in *Griswold* in which he held:

> "*He does not believe that we are granted power by the Due Process Clause or any other constitutional provision or provisions to measure the constitutionality of the arbitrariness of any legislation by their notions of civilised standards of conduct*. *This is because the appraisal of legislation is the power to make laws, not the power to interpret them"*.[212]

[209] 410 U.S. 113 (1973).
[210] 405 U.S. 438 (1972).
[211] *Roe v. Wade*, 410 U.S. 113, 173-74 (1973).
[212] Supra note 145, 381 U.S. at 509. Similar dissenting opinion was also seen by Justice white in *Doe v. Bolton* wherein he held that such an issue should be left with the people and to the political processes the people have devised to govern their affairs, 410 U.S. 179, 222 (1973) (Justice White dissenting).

Apart from the dissenting opinions in *Roe*, *Griswold* or *Doe*, several U.S. cases conceded that Privacy was not a right recognised by drafters of the Constitution but rather a judicially created right. For instance, *Maher v. Roe*[213] reiterated the doctrinal component that for social issues like marital Privacy or freedom to terminate the pregnancy, judicial legislation could not be the last resort and should be entrusted to the legislative and executive branches. The Court in *Ferguson v. Skrupa*[214] terms it as the 'policy of judicial nonintervention':

> *"When an issue involves policy choices as sensitive as those implicated by public funding of abortions, the appropriate forum for their resolution in a democracy is the legislature."* [215]

Now, turning away from the question of nature and source of Privacy, there is also much debate around whether protection of rights like marital Privacy or freedom to terminate the pregnancy even encompass the notions of autonomy, dignity, or individuality, including personhood; therefore, right to privacy. The Supreme Court of India has also gone along the lines of the abovementioned Western judgements, which include home and all its activities in the private sphere. For instance, the Supreme Court of India in *Gobind v. State of M.P.*[216] explained the right to privacy as:

> *"Any right to privacy must encompass and protect the personal intimacies of the home, the family, marriage, motherhood, procreation and child-rearing"*[217]

According to Gautam Bhatia, such conceptualisation of Privacy by the Supreme Court is ambiguous or obscure.[218] He says that while defining Privacy, the Court intermixes three concepts of Privacy, i.e., spatial, institutional, and decisional Privacy. The word '*home*' in the above-said quote in *Gobind* denotes that an individual has the Right to Privacy within the territories of their home, explicitly moving on to the functions performed inside the said territory, i.e., marriage procreation. Also, the home can be read as a '*household*,' i.e., as an institutional concept that

[213] 432 U.S. 464 (1977).
[214] 372 U.S. 726 (1963).
[215] Ibid, 372 U.S. at 479-80.
[216] *Gobind v. State of M.P.*, (1975) 2 SCC 148.
[217] Ibid, pp. 24.
[218] Bhatia, G. (2017). The Constitution and the Public/Private Divide: *T. Sareetha* v. *Venkata Subbaiah*. *Sareetha v. Venkata Subbaiah (July 30, 2017)*.

provides a sanctuary to activities mentioned in the Court's opinion. The said activities are also a result of decisions core to an individual's life which should be insulated from the State's interference, and in this sense, reflect decisional autonomy. Such privacy protections within the household and its activities originate in the personal laws where ancient texts and customs, particular to a specific caste or religion, dictate the codification of law and what judicial rulings should adhere to.[219] The activities are considered sacrosanct to a particular community, advocating for its autonomous existence and, therefore, free from interference by the state. It can be seen through an intense debate in the aftermath of Justice Pinhey's judgement in the case of *Rakhmabai*. The statute in contention was the Hindu Marriage Act, which restores conjugal rights. *Rakhmabai* argued that Section 9 of the said Act forces restitution as the last opportunity given before the breakdown of the marriage and a precondition of divorce, and therefore violates the life and liberty of an individual under Article 21 of the Indian constitution. A similar plea was also made in the case of *T. Sareetha v. Venkata Subbaiah*,[220] where the court's eloquence is worth noting:

> *"The purpose of a decree for restitution of conjugal rights is to coerce through the judicial process the unwilling party to have sex against the person's consent and free will. Relying on Griswold and Roe, sexual expression is so integral to one's personality that it is impossible to conceive of sexuality on any basis except based on consensual participation"*.

However, the Supreme Court overruled the majority opinion of *T. Sareetha* in the case of *Saroj Rani v. Sudarshan Kumar*, where Section 9 was considered constitutional by stating that conjugal rights serve a social purpose preventing the breakup of the marriage and do not force sexual consummation. On the one hand, the Courts in *Sareetha* and *Rukhmabai* put forward reformist views around 'marital privacy', which prioritise decisional Privacy over spatial and institutional Privacy based on unequal power structures within a family. Moreover, on the other side are decisions like Saroj Rani, which consider the institution of marriage as sacrosanct on the premise that personal laws do not constitute law and therefore do not fall within the judicial purview.[221]

---

[219] Personal laws are laws which govern the family, gender relations, marriage, divorce, inheritance, and so on, as represented by the court in *Gobind*, supra, note 48.
[220] AIR 1983 Andhra Pradesh 356.
[221] Personal laws do not constitute law under Article 13 of the constitution and for the purposes of the fundamental rights chapter. The reasoning behind it of the court in *State of Bombay v. Narasu Appa Mali, AIR 1952 Bom 84* is that personal laws are derived from scripture and not through any legislation.

What the latter set of decisions forget is that the State itself enforces the personal laws, and thus the private sphere of the home or marital life is also defined and constructed by legislation and active enforcement by the State.[222] Thus, there is a potential for the State to interfere with the decision, related to spatial and institutional autonomy, even in the case of personal laws, that should be subjected to judicial scrutiny for privacy protection. These cases seem to blur the public/private divide as they prove that even within the private sphere of the home, there can be non-consenting activities that demand privacy protection.

1.5. Intimacy

According to Alan Westin, intimacy is one of the four states of Privacy that reflects the extent and nature of an individual's involvement in the public sphere.[223] Westin states that intimacy refers not merely to intimate relations between spouses or partners, but also between friends, family, and colleagues. The theory of intimacy moves beyond other conceptions, like secrecy and limited access, as it does not pay attention to individual self-creation and gives equal weightage to human relationships. Intimacy can also be located within the defence of personal (spousal relationship) and professional (attorney-client) privileges given globally by the courts during testimonies. The laws protect their intimate communications primarily for two reasons: a) protection from embarrassment from secrets being revealed to the public, and b) breach of trust and confidentiality.[224] Concerning these reasons, intimacy overlaps with the secrecy and limited access conception. However, it also moves beyond those conceptions and protects personal loyalties even in cases where states compel disclosure. Orders to compel testimony have been protected through privileges as there might be a consequence of an invasive disclosure affecting individuals and a collective group of individuals. Instead, in the case of intimacy, individual interests and collective interests should be understood as one. Society as a collection of individual relationships runs on implied rules regarding communication activities, which benefit the entire community.

Such relationships are not specific to spousal or partner relationships but also extend to friendship or kinship. As Peter Berger asserts, "*If there is one universal, indeed primaeval, principle of morality, it is that one must not deliver one's friends to their enemies*".[225] E.M. Forster considers

[222] Supra note 175, p. 29.
[223] Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, *25*(1), 166.
[224] Radin, M. (1927). The privilege of confidential communication between lawyer and client. *Calif. L. Rev.*, *16*, 487, p. 492-93.
[225] Berger, Now, 'Boat People' From Taiwan, New York Times, Feb. 14, 1978, at 35, col. 4.

personal relationships like friendship necessary to human life and affirms that it is essential not to disclose communications and activities to 'not let down' the relationship.[226] Similarly, in the case of kinship, Professor Kanodian calls for a constitutional right in the individual to place loyalty to parents over loyalty to the state.[227] The constitution's fifth amendment protects against compelling to testify for any 'infamous crime'. In the case of *In Re Agosto*, the Court granted the son the privilege not to testify against his father, who was involved in organised crime, thus recognising kinship privilege.[228] Thus, individual reliability is critical in relationships which is not contractual as in business relationships.

In Indian jurisprudence, the Indian Evidence Act has shades of personal and professional communications, which aims to protect communications during the marriage, and state affairs, attorney-client privilege, and official communications.[229] As pointed out above, intimate relationships are always interpersonal relationships, i.e., there is a sense of caring involved, which the said Act seems to protect too. Jeffrey Reiman defines interpersonal relationships through an example, "*one ordinarily reveals information to one's psychoanalyst that one might hesitate to reveal to a friend or lover. That hardly means one has an intimate relationship with the analyst*".[230] Reiman declares that what is missing is "*the particular kind of caring that makes a relationship not just personal but intimate*".[231] Herein, it needs to be understood that every spousal relationship does not involve love, liking, or caring, and therefore intimate relationships are highly subjective. Similarly, certain relationships are not considered 'intimate' in their strictest sense yet fall within the bracket of the private sphere and demand intimacy, i.e., protection from the State. Thus, conceptualising the scope of intimacy is crucial and further contextual to the type of relationship.

Each dimension of Privacy discussed above produces innumerable insights and furthers the conceptualising privacy query. However, as Daniel Solove states, settling on one interpretation would '*result in either a reductive or broad account of privacy*'.[232] Although privacy has overlapping

[226] Forster, E. M. (1972). Two Cheers for Democracy. 1951. *London: Edward Arnold*, p. 66.
[227] Kandoian, E. (1984). The Parent-Child Privilege and the Parent-Child Crime: Observations on State v. DeLong and In re Agosto. *Me. L. Rev.*, *36*, 59.
[228] 553 F. Supp. 1298, 1331 (1983).
[229] Refer to Section 122 - Section 129 of the Indian Evidence Act. Section 122 pertains to communication during the marriage, Section 123 applies to persons not to give any evidence that may be derived from any unpublished records, Section 124 pertains to official communications, and Section 126 applies to barrister/attorney/pleader, not to disclose any communication made to him by this client.
[230] Reiman, J. H. (1976). Privacy, intimacy, and personhood. *Philosophy & Public Affairs*, 26-44, p. 35.
[231] Ibid.
[232] Solove, D. J. (2002). Conceptualising privacy. *California law review*, p. 1124.

conceptions, Part A distils specific dimensions of privacy to put forward varied perspectives in the existing literature. It leaves us with certain components that constitute privacy by simultaneously stating that there cannot be a common definition of privacy cutting across geographies and cultures. The discussion points towards focusing on the context within which intimacy or secrecy is required, and utilising a framework that aids contextual examination. Before providing an answer to the first question, Part B is a pragmatic attempt to conceptualise Informational privacy by providing an account of the Indian jurisprudence. Informational privacy deserves to be discussed separately for the following reasons: First, it is a central theme of this thesis, and second, as shown in the following sub-parts, it encapsulates the different conceptions of privacy discussed above. Part C will provide the answer to examine the context in which a right to privacy needs to be safeguarded.

PART B - CONCEPTUALISING INFORMATIONAL PRIVACY

Around 130 years ago, Warren and Brandeis, in their piece, discussed the impact of the press on the diminishing boundaries of propriety and decency due to their increasing intrusion into an individual's life. With rapid technological advancements in surveillance, the intensity and complexities of life have increased, which demands much more solitude and Privacy from physical and mental invasions.

2.1. PRE-*GOBIND* JURISPRUDENCE

Informational Privacy has been implanted as a constitutional right to Privacy by the judiciary in India. The right to Informational Privacy in India has emerged as a product of judicial activism and expansion of constitutional rights manifested through the interpretation of Article 21 and Article 19 of the Indian Constitution. To understand the expansion of such rights, we need to examine the ratio decidendi of *M.P. Sharma,*[233] and *Kharak Singh*[234] that held the Right to Privacy cannot be read directly into the phrase 'liberty' under Article 21, embracing a literal interpretation of the Constitution. The issue the Court considered in *M.P. Sharma* was whether the search and seizure of documents from the custody of a person amounted to a violation of Article 20(3) of the Indian Constitution - Self-Incrimination. The origin of self-incrimination can be traced back to the fifth amendment of the U.S. Constitution,[235] which the Court stated is not analogous to the Right to

[233] *M.P. Sharma & Others v. Satish Chandra & Others*, AIR 1954 SC 300.
[234] *Kharak Singh v. State of U.P. & Others*, AIR 1963 SC 1295.
[235] "No person ……. shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law …"

privacy implied in the fourth amendment of the US constitution.[236] The Court refused to agree with *Boyd v. United States*, which included the Right to Privacy as part of self-incrimination because if constitution-makers have not made any provision analogous to the fourth amendment, the Court has no ground to read and give into effect such a right.[237] Only in this context the Court briefly refers to the Right to Privacy, indicating a textual interpretation of the Constitution. Thus, the relationship between Article 20(3) and the Right to Privacy was not directly questioned before the Court but was purely incidental to the discussion. Therefore, the conclusion that the Court in *M.P. Sharma* did not recognise the fundamental Right to privacy does not hold water, as the decision was only in the context of self-incrimination.

Before the Court in *Kharak Singh*, the question was about the constitutionality of Police Regulations in Uttar Pradesh. Section 236 of U.P. Regulations provided inter alia surveillance powers via secret picketing of the house, domiciliary visits, and shadowing 'history sheeters' (repetitive criminals) to record all the places they visit, people they visited as contacts and all their contact movements. In the context of such regulations, the Court was called upon to examine the scope of 'personal liberty' guaranteed under Article 21 and freedom of movement under Article 19(1)(d). The majority opinion stated that the expression of personal liberty under Article 21 includes all rights that make up the personal liberties of man other than those dealt with or expressed in several clauses of 19(1). By compartmentalising the freedoms, the Court interpreted Article 21 as a provision containing the "residue" of rights left out from Article 19, and domiciliary visits violate liberty guaranteed under Article 21.[238] Thus, *Kharak Singh* points towards two conclusions - incongruent with each other. On the one hand, the Court accepts the maxim that "*every man's house is his castle*", and any incursion violates personal liberty. On the other hand, it states that due to an absence of an explicit provision in the Indian Constitution akin to the fourth amendment, the Right to privacy cannot be imported within the conceptualisation of liberty.

[236] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized."
[237] *Boyd v. United States*, 116 US 616 (1886).
[238] Gautam Bhatia, "*The Right to Privacy and the Supreme Court's Referral: Two Constitutional Questions*", August 11, 2015, Indian Constitutional Law and Philosophy. Available at https://indconlawphil.wordpress.com/2015/08/11/the-right-to-privacy-and-the-supreme-courts-referral-two-constitutional-questions/ (Accessed on 19th January, 2021).

Furthermore, the fact that it was not the intention of the constitution-makers to include the Right to Privacy is partially actual, as shown in Benegal Shiva Rao's *The Framing of India's Constitution* - also used by Rahul Matthan in his book *Privacy 3.0*. Rao's extensive collection of constituent assembly debates shows the first reference to the Right to Privacy in KT Shah's '*Note on Fundamental Rights*', which explicitly mentions the liberty of the person and the Privacy of the home as the most essential and indispensable rights for human existence. Dr B.R. Ambedkar - considered to be the principal architect of the Indian Constitution - in his draft of 24th March 1947, also formulates the Right to Privacy as

> *The Right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures shall not be violated. No warrants shall issue but upon probable cause, supported by oath or affirmation and particularly describing the place to be searched and the persons or things to be seized.*

Although there were strong dissents in the Constituent Assembly, Alladi Krishnaswamy Ayyar and B.N. were the most vocal critics. Rau's concern was mainly regarding the Right to Privacy as not being explicitly included as part of fundamental rights as it will lead to complications in the administration of Justice.[239] The discussion ended with the amendment being defeated through voting with little deliberation. It would be safe to presume that in those times, the home and correspondence were considered sacred precincts where an individual could demand secrecy - drawn from the fourth amendment of the US Constitution. Therefore, it remains imperative for the legislature and judiciary of a particular time to be cognizant and anticipative of contemporary societal developments and formulate privacy jurisprudence. Considering this argument, *M.P. Sharma* and *Kharak* are not considered good law but mark the starting point of the discussion around privacy within the Indian judiciary.

The transition from a rigid approach to fundamental rights in *MP Sharma* and *Kharak* to the flexible balancing between privacy, democracy, and other interests' approach in *Gobind*, *Malkani* and *PUCL* marks the starting point where informational Privacy germinated in India's jurisprudence. The argument that whatever is not explicitly mentioned in the Constitution is not a part of it is too primitive an understanding against the settled canons of Constitutional Interpretation. If such had

[239] Arvind Pillai & Raghav Kohli, A case for a customary Right to Privacy of an Individual: A Comparative Study on Indian and other State Practice, (2017) Oxford U Comparative L Forum 3 at ouclf.law.ox.ac.uk.

been the interpretation method, fundamental freedoms like the Right to Education,[240] Right to a clean environment,[241] Right to a speedy trial,[242] Right to go abroad, and right to protect one's reputation would not have existed within the phrases 'Life' and 'Liberty' under Article 21. These cases serve as precedents for implying logical interpretations of a statute which is silent in certain aspects. Such implication follows the statute's overall purpose and is further ascertained from the overall scheme of the legislation.

2.2. GOBIND, MALAK SINGH & PUCL: WATERSHED MOMENT IN INDIA'S INFORMATIONAL PRIVACY JURISPRUDENCE

Gobind[243] is considered the watershed moment for establishing a Right to Privacy in Indian jurisprudence. *Gobind* dealt with analogous facts to those in an instance such as *Kharak*, where Regulations 855 and 856 of State Police Regulations were in question under which a history-sheeter was under surveillance. Justice Mathew, who delivered the judgement, relying on the U.S. Supreme Court's decision in *Griswold*, stated for the first time that the Indian Constitution recognises a '*Right to be Let Alone*. However, while discussing the validity of the impugned regulations, the Court stated that the Right to Privacy is not an absolute right so that it can be curtailed in the presence of a valid law. In *Gobind*, the Court found that Section 46(2)(c) of the Police Act provides a valid statutory backing, i.e., preventing the commission of offences targeted at repeat offenders, making the Surveillance Act legitimate.

The judgement in *Gobind* stands as noteworthy for two reasons: Although it does not provide a specific meaning of Privacy, it agrees with the U.S. cases of *Griswold* and *Roe*, noting that there are multiple zones of Privacy, each having its distinctive characteristic. Thus, the concept of Privacy cannot be funnelled down to a single provision within the Constitution. *Second*, it provides a constitutional framework for legalising surveillance by noting that a good law can impose a reasonable restriction on a fundamental right based on a '*compelling public interest*'. It is important to distinguish here that 'public interest' is also a ground for reasonable restriction under Article 19 of the Constitution, but the Court's interpretation has never encompassed the word 'compelling' within its meaning. Thus, through *Gobind*, a stricter standard has been placed upon finding

[240] *Mohini Jain v. State of Karnataka*, (1992) 3 SCC 666.
[241] *M.C. Mehta v. Kamal Nath*, (2000) 6 SCC 2013.
[242] *In Re. Hussainara Khatoon & Ors. v. Home Secretary, Bihar* (1980) 1 SCC 81.
[243] (1975) 2 SCC 148.

potential Article 21 violations (including privacy violations) than Article 19 violations.[244] The justification of compelling public interest can be traced back to First Amendment rights precedents of the US Constitution, the first being Justice Frankfurter's concurrence to *Sweezy v. New Hampshire*.[245] Justice Frankfurter's ruling against the government and quashing the contempt conviction held:

> *When weighed against the grave harm resulting from the government intrusion into the academic life of a university, the government's justification for compelling a witness to discuss the contents of his lecture appears grossly inadequate.*[246]

Therefore, under the compelling public interest argument, the balance of conflicting interests, i.e., the Government's intrusion concerning the civil liberties of a citizen, is called into question. Though *Sweezy* is primarily a freedom of speech precedent, Frankfurter's concurrence notes elements of what Stephen A. Siegel noted as '*political privacy*'[247] or inviolability of the Right to privacy in political thoughts, actions and associations. Frankfurter notes,

> *"For a citizen to be made to forgo even a part of so basic a liberty as his political autonomy, the subordinating interest of the State must be compelling…. However, the inviolability of privacy belonging to a citizen's political loyalties has so overwhelmed an importance to the well-being of our kind of society that it cannot constitutionally encroach upon the basis of so meagre a countervailing interest of the State as may be argumentatively found in the remote, shadowy threat to the security of New Hampshire…. In the Political realm, as in the academic, thought and action are presumptively immune from inquisition by political authority…."*[248]

Thus, whether the *Gobind* bench knew it at the time or not, it incorporated the compelling interest test under Article 21 of the Indian Constitution, which means the Government must demonstrate

[244] Bhatia, G. (2014). State Surveillance and the Right to Privacy in India: Constitutional Biography. National Law School of India Review, 26(2), 127-158.
[245] 354 U.S. 234 (1957). Sweezy was a professor at the University of New Hampshire who refused to answer the questions by Hampshire's Attorney General about his classroom lectures and his involvement in subversive practices with the Progressive Party. Thus, there was a contempt proceeding against Sweezy demanding protection of First Amendment values under the US Constitution.
[246] Ibid, at 261.
[247] Siegel, S. A. (2006). The origin of the compelling state interest test and strict scrutiny. *American Journal of Legal History*, *48*(4), 355-407, p. 365.
[248] Supra note 245, at p. 365 & 366.

a compelling public interest to justify any act of surveillance. Soon after *Gobind*, *Malak Singh v. State of Punjab & Haryana*, arose, wherein two individuals challenged the constitutionality of Rule 23 of the Punjab Police Rules that there was no ground to surveil, intercept or suspect them of being history-sheeters.[249] The Court embarked upon a lengthy discussion on the balancing of prevention of crime by the State and the Right of liberty of individuals while listing out the scope and limitations of police surveillance:

> *"Permissible surveillance is only to the extent of a close watch over the movements of the person under surveillance and no more. So long as surveillance is to prevent crime and is confined to the limits prescribed by Rule 23.7, we do not think a person whose name is included in the surveillance register can have a genuine case for complaint."*

The Court noted that interference follows the law and the prevention of disorder and crime are recognised as exceptions, even by the European Convention of Human Rights (ECHR), i.e. the Right to respect a person's private and family life.[250] It is important to note here that *Malak Singh* allows '*targeted*' surveillance of a person's movements without any illegal interference, i.e. gathering data on a limited set of people whose name is mentioned in the police registers as repeat offenders or serious criminals. The Court went on to elaborate on the contours of '*illegal interference*',

> *But all this does not mean that the police have a license to enter the names of whomever they like (dislike?) in the surveillance register, nor can the surveillance be such as to squeeze the fundamental freedoms guaranteed to all citizens or to obstruct the free exercise and enjoyment of those freedoms; nor can the surveillance so intrude as to offend the dignity of the individual. Surveillance of persons who do not fall within the categories mentioned in Rule 23.4 or for reasons unconnected with the prevention of crime or excessive surveillance falling beyond the limits prescribed by the rules will entitle a citizen to the court's protection which the court will not hesitate to give.*

[249] (1981) 1 SCC 420.

[250] "(1) Everyone's right to respect for his private and family life, his home and his correspondence shall be recognised. (2) There shall be no interference by a public authority with the exercise of this right, except such as is in accordance with law and is necessary in a democratic society in the interests of national security, public safety, for the prevention of disorder and crime or for the protection of health or morals."

Thus, the Court reiterated the view in Gobind that the Right to Privacy is not absolute and is subjected to certain lawful & reasonable restrictions like prevention of crime or disorder, public morals, public health and the rights and freedoms of others. All the earlier cases discussed have one thing in common: they are explicitly discussing the existence of a Right to privacy in the Indian Constitution and whether it can be granted as a guaranteed fundamental right. *PUCL v. Union of India,* while taking note of earlier decisions, laid down guidelines for the executive's power of exercising surveillance to curb its misuse. [251] While *Kharak*, *Malak,* and *Gobind* conceptualised Privacy in the physical realm, *PUCL* included protecting personal communications and safeguarding citizens from arbitrary state interference.

PUCL was public interest litigation opposing the excesses of the then-political regimes abusing their power to carry out arbitrary telephone tapping. In *PUCL*, Section 5(2) of the Indian Telegraph Act of 1885 was constitutionally challenged, claiming it breached Article 21 and Article 19(2) of the Constitution.[252] Justice Kuldip Singh's judgement notes that telephone conversations hold an intimate character and are an essential ingredient of a person's privacy, and therefore tapping of such conversations infringes Article 21 unless permitted by law:

> *"Whether the right to privacy can be claimed or has been infringed in each case would depend on the facts of the said case. However, the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as a "right to privacy". Conversations on the telephone are often of an intimate and confidential character. Telephone conversation is a part of modern man's life. It is considered important that more and more people carry mobile telephone instruments in their pockets. Telephone conversation is an important facet of a man's private life. Right to privacy would*

[251] (1997) 1 SCC 301.

[252] **5. Power for the Government to take possession of licensed telegraphs and to order interception of messages.** On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order:
Provided that press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this subsection.
For Telegraph Act, 1885, Refer to https://dot.gov.in/act-rules-content/2442.

> *certainly include telephone conversations in the privacy of one's home or office. Telephone Tapping would, thus, infract Article 21 of the Constitution of India unless it is permitted under the procedure established by law.'*[253]

The expression '*procedure established by law*' constitutes two preconditions, i.e., "public emergency" or "interest of public safety", and five grounds to intercept a transmission, i.e., a) Sovereignty and Integrity of India, b) security of the State, c) Friendly relations with foreign states, d) public order, e) preventing incitement to the commission of an offence. In light of such vague grounds, it is essential to note here that the "*procedure which deals with the modalities of regulating, restricting or even rejecting a fundamental right falling within Article 21 has to be fair, not foolish, carefully designed to effectuate, not to subvert, the substantive right itself*".[254] The Court in *PUCL* stated that the two preconditions - *"that take their colour off each other"* - are not secretive, but rather should be apparent to a reasonable person. Herein, the Court tries to proportionately balance an individual's Privacy with the risk posed to the public or their interests. Because of the absence of rules providing safeguards to prevent interception/disclosure of messages, the Court directed to construe the provisions of Article 21 (where 'privacy' has been interpreted to reside impliedly) per Article 17 of the International Covenant on Civil and Political Rights[255] or Article 12 of the Universal Declaration of Human Rights.[256] Following such interpretation, the Court went on to lay down measures for telephone tapping orders, including: a) Orders for telephone tapping may only be issued by the Home Secretary of the Central or State Government, b) Before making the order, the authority shall decide whether telephone tapping is the last resort or the information can be acquired through less intrusive means, c) Orders shall be valid for two months from the date of the issue, d) Review Committees shall be constituted of secretary-level officers who shall be in charge of compliance with law or destruction of copies of intercepted communications, and e) an obligation is on the issuing authority to maintain records of communication.

---

[253] Supra note 251, at p. 311, pp. 18.
[254] *Maneka Gandhi v. Union of India*, AIR 1978 SC 597.
[255] Article 17 - 1. 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. 2. Everyone has the right to the protection of the law against such interference or attacks.
[256] Ibid.

The *PUCL* judgement came at the dawn of mobile telephony, wherein the Court observed that "*more and more people are carrying out mobile in their pockets*",[257] and thus it demands the necessity to frame parliamentary legislation protecting citizens' informational Privacy. It should be noted that judicial scrutiny is not mentioned in the measures propounded in *PUCL*. Despite the argument made by the petitioners, prior judicial scrutiny of telephone tapping is the only way to safeguard privacy rights. The Court, in this regard, takes note of the English Interception Act, 1985 - the precursor to the *Regulation of Investigatory Powers Act* (RIPA), 2016 - and leaves it to the executive branch to introduce judicial scrutiny of surveillance powers through legislation.

The discussion of *PUCL* was necessary for two important reasons: a) *First*, *PUCL* 1997 guidelines, though specifically related to telecommunication surveillance, also influenced the Information Technology Act (I.T. Act) (2000) and the underlying rules, meant for potentially all contemporary digital communications, b) *Second*, the two preconditions established under the telegraph act, that of *public safety* and *public interest*, seem to be absent from the I.T. Act, signaling the lower threshold for surveillance, post-legislative enactment. Both reasons are discussed in detail in the following subsection to analyse the legislation and advance the conceptualisation of informational privacy in the contemporary age.

2.3. POST-PUCL DEVELOPMENT OF INFORMATIONAL PRIVACY JURISPRUDENCE

The construction of informational Privacy in *PUCL* settles the narrow grounds of state interest for privacy infringement. Though the safeguards were strengthened versions, the Court declined to insert judicial scrutiny of the interception requests. The Court left the gatekeeping requirement to the executive branch, aligning with the separation of powers doctrine. The significant lacunae of *PUCL* are its ignorance of the conflict of interest of the executive, which is responsible for both surveillance and deciding upon its legality. *PUCL* guidelines can be compared with RIPA, which empowers the Secretary of State to issue a warrant for phone-tapping in three cases, i.e. national security, preventing or detecting serious crime, and the economic well-being of the U.K.,[258] which

[257] Supra note 251, pp. 18.

[258] S. 20 - **Grounds on which warrants may be issued by Secretary of State -** A targeted interception warrant or targeted examination warrant is necessary on grounds falling within this section if it is necessary— a) in the interests of national security, (b) to prevent or detect serious crime, or (c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security (but see subsection (4)).

the Judicial Commissioner further approves under Section 23-25.[259] It denotes the intention of the U.K. legislators first to insert minimal grounds for the interception to protect against intrusion of Privacy, as opposed to five grounds and two sub-conditions in the Indian legislation and *second*, maintain checks and balances on executive power.

In the series of precedents, *District Registrar and Collector, Hyderabad v. Canara Bank,* a 2005 judgement holds importance due to its express recital that "*privacy deals with persons and not places*".[260] The Court herein dealt with Section 73 of the Indian Stamp Act, 1899, which empowered public officers to inspect registers, books, records, papers, and documents in their custody at all reasonable times.[261] So, the question before the Court was twofold: a) whether collector's power in section 73 to authorise 'any public officer' to inspect or extract inter alia documents is an excessive power? and b) Does the search and seizure of a customer's documents voluntarily in possession of a bank under Section 73 violate the Right to Privacy? While answering the first issue, the Court held that Section 73 suffers from the excessive delegation and stated:

> *"The impugned provision in sec. 73 enabling the Collector to authorise 'any person' whatsoever to inspect, to take notes or extracts from the papers in the public office suffers from the vice of excessive delegation as there are no guidelines in the Act and more importantly, the section allows the facts relating to the customer's privacy to reach non-governmental persons and would, on that basis, be an unreasonable encroachment into the customer's rights. This part of Section 73 permits delegation to 'any person' who suffers from the above serious defects and, for that reason, is, in our view, unenforceable. The State must clearly define the officers by designation or state that the power can be delegated to officers not below a particular rank in the official hierarchy, as may be designated by the State."*

[259] Ibid, Section 23, **Approval of warrants by Judicial Commissioners**: a) In deciding whether to approve a person's decision to issue a warrant under this Chapter, a Judicial Commissioner must review the person's conclusions as to the following matters — (a) whether the warrant is necessary on relevant grounds (see subsection (3)), and (b) whether the conduct that the warrant would authorise is proportionate to what is sought to be achieved by that conduct.

[260] *District Registrar and Collector, Hyderabad v. Canara Bank,* AIR 2005 SC 186.

[261] Section 73 of the Indian Stamp Act - "Every public officer having in his custody any registers, books, records, papers, documents or proceedings, the inspection whereof may tend to secure any duty, or to prove or lead to the discovery of any fraud or omission to any duty, shall at all reasonable times permit any person authorised in writing by the Collector to inspect for such purpose the registers, books, papers, documents and proceedings, and to take such notes and extracts as he may deem necessary, without fee or charge."

The Court's opinion to the second question is equally insightful and explanatory where it notes:

> *"The right to privacy deals with 'persons and not places', the documents or copies of documents of the customer which are in a Bank, must continue to remain confidential vis-a-vis the person, even if they are no longer at the customer's house and have been voluntarily sent to a Bank. If that is the correct view of the law, we cannot accept the line Miller in which the Court proceeded on the basis that the right to privacy is referable to the right of 'property' theory. Once that is so, then unless there is some probable or reasonable cause or reasonable basis or material before the Collector for reaching an opinion that the documents in possession of the Bank tend to secure any duty or to prove or to lead to the discovery of any fraud or omission concerning any duty, the search or taking notes or extracts therefore, cannot be valid. The above safeguards must be read into the search, inspection, and seizure provision to save it from any unconstitutionality."*

It is essential to carefully examine the two observations and how they advance informational privacy's meaning. As discussed above, the Right to privacy under Article 21 is not absolute and can only be infringed according to the phrase '*procedure established by law*'. Various supreme court judgements have described the word 'procedure' as something which should be fair, just and reasonable.

While dealing with the first question of law on excessive delegation, the Court objects to the arbitrariness by which a public official can encroach on an individual's privacy. The arbitrariness is constitutionally problematic due to the absence of guidelines for any public officer under section 73 of the Indian Stamp Act. The '*any registers*', '*secure any duty*', '*permit any person*' and '*take such notes and extracts as he may deem necessary*' seems to provide a public officer with unbridled, ambiguous, and vague authority amounting to a breach of an individual's informational privacy. Herein, the Court, while noting the American jurisprudence in depth - specifically alludes to what Justice Stevens held in *Whalen v. Roe:*[262] *The Right embraces a general individual interest in avoiding disclosing personal matters* and '*interest in independence in making certain kinds of important decisions*. Herein, the Court holds the statute unconstitutional for the first time because it abuses individuals' privacy rights.

[262] (1977) 429 US 589.

Holding the above-stated second question, where the Court states that the '*right to privacy deals with persons and not places*', also requires a thoughtful discussion. Herein, the Court discusses the privacy rights vis-a-vis a third party, i.e., the Bank and whether the State can have unrestricted access to obtain the information in possession of the Bank. The Court held that:

> "*Once we have accepted in Govind and it latter cases that the right to privacy deals with persons and not places, the document or copies of documents of the customer which are in Bank, must remain confidential vis-a-vis the person, even if they are no longer at the customer's house and have been voluntarily sent to a bank*".

By accepting the Gobind argument, the Court in Canara rejects the proletarian foundation of Privacy while accepting the Privacy of persons. For such purposes, the Court also relies on American jurisprudence - most notably, the judgements in United States v. Miller[263] and *Katz v. United States*.[264] In the landmark case of *Katz v. United States,* the Government obtained evidence against a suspect by attaching an electronic listening device to the top of a telephone booth. The Court stated that the discussion of whether a telephone booth is a constitutionally protected area deflects the attention from the individual claim of the Right to privacy, as the Fourth Amendment of the U.S. Constitution protects people, not places. While discussing the voluntary sharing of information, the Court made the following observation:

> *"But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. What the individual sought to exclude when he entered the booth was not the intruding eye but the uninvited ear……. The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a "search and seizure" within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the booth wall can have no constitutional significance.*"

However, the majority opinion in *Miller* establishes the narrower conception of the reasonable expectation of privacy test by holding that once a person passes on the cheque to a bank, it loses

[263] 425 U.S. 435.
[264] 389 U.S. 347 (1967).

the privacy rights protection under the fourth amendment. Herein *Miller* lays down a new principle, i.e., '*assumption of risk*', which means that the '*depositor takes the risk, in revealing his affairs to another*' wherein it cannot enjoy a reasonable expectation of privacy. In essence, *Miller* makes a stringent argument in finding a reasonable expectation and opens doors for much more rampant search and seizure than was previously permitted per *Katz*. *Smith v. Maryland* also reaffirmed the limits on the Government's access to stored records.[265] It presented a similar question to *Katz* regarding installing a pen register - a device that creates a list of numbers dialled from a telephone. The majority opinion held that there was no reasonable expectation of Privacy as the petitioner voluntarily provided the telephone company's information. However, in his dissenting opinion, Justice Stewart believed that no one would be happy to broadcast the list of telephone numbers one has dialled, thus revealing the most intimate details of one's life. It is like Justice Brennan's dissenting opinion in *Miller* that note, "*an individual cannot participate in the economic life of modern society without maintaining a bank account…. Moreover, to permit the third party to share the information with the Government allows the Government to misuse or abuse their powers"* (emphasis supplied).[266] Cheques are not merely negotiable instruments but reveal an individual's personal information (like with whom one is spending money and how frequently this is spent). Saying that one assumes a risk by opening a bank account and therefore has no claim in Privacy is insensitive and illogical. The dissenting opinions in *Miller* and *Smith* and the majority opinion in *Katz* are ones to which the Indian Supreme Court in *Canara* adheres. It rejects the argument that once the customer assumes the risk of conveying the information to the third party, it loses the Right to claim Privacy.

The significance of the judgement in *Canara* lies in rejecting the possibility of arbitrarily searching and seizing the documents in the custody of an individual. However, *Canara* should also be viewed as recognising informational Privacy and laying down the foundations of its regulation. Herein the Court revisits Section 73 of the Act reading, which denotes that no person shall receive any benefits from any instrument which is not duly stamped. It also allows the public officer to impound such instruments and recover the penalty for the interest of the revenue. However, there need to be guidelines that authorise the public officer and its actions under the Act. Without such guidelines, any search and seizure of the instrument under the said Act amount to a disproportionate act as regards the reasonable nexus between the purpose sought to be achieved and the stringency of the provider cease to exist.

[265] *Smith v. Maryland*, 442 U.S. 735 (1979).
[266] Ibid, at 447.

Though *Canara* laid down the foundation of 'informational privacy', the 2017 judgement of *K.S. Puttaswamy v. Union of India* cemented its contours.[267] Also, it is important to note herein that *Puttaswamy* being a larger bench (9-judge bench), overruled *M.P. Sharma* (1954 - 8 judge bench) and *Kharak* (1962 - five-judge bench) to the extent that the Right to privacy is not protected under the Constitution, and thereby effectively upholding Right to Privacy as a fundamental right, for the first time in Indian jurisprudence.[268] In addition to the Right to Privacy getting explicitly recognised, the majority opinion of *Puttaswamy* needs to be examined because of Justice Chandrachud's heavy focus on informational privacy. He juxtaposes Privacy in today's digital economy, discusses the dangers of data mining and orders the need for an adequate data protection law. His opinion refers to the positive and negative obligations of the State towards individuals' rights, the latter restricting the interference of the Government while the former creates an obligation to frame a legislative framework.[269]

The Right to Privacy recognises the inviolable right to choose and express oneself free from interference. Until *Puttaswamy,* the test for privacy infringement was implicit and evolved on a case-by-case basis. The judicial interpretation of '*procedure established by law*' under Article 21 was interpreted as 'fair, just & reasonable' or 'a compelling state interest' to justify the infringement of privacy rights. Justice Chelameswar notes the reason behind such varied interpretations of the phrase and the lack of a consistent test to justify infringement.[270] He reasons that Privacy is not an independent right but a constituent of freedoms across the spectrum of the Indian Constitution. He supports it with the fundamental Right to equality under Article 14, which guarantees protection from any arbitrary or unreasonable state interference that causes discrimination among individuals. Similarly, the Right to Privacy is a constituent of freedom of speech and expression that allows an individual to express themselves in whatsoever manner and remain silent. However, as Justice Chelameshwar points out, no freedom is absolute and subjugated to reasonable restrictions, which also applies to the Right to Privacy.[271] He meant that it depends on which provision the claim of Privacy emanates, and accordingly, the standard for its justification will also emerge.

---

[267] *K.S. Puttaswamy v. Union of India*, AIR 2017 SC 4161.
[268] *M.P. Sharma v. Satish Chandra*, (1954) 1 SCR 1077, *Kharak Singh v. State of Uttar Pradesh and Ors.*, AIR 1963 SC 1295.
[269] Bhandari, V., Kak, A., Parsheera, S., & Rahman, F. (2017). An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict. *IndraStra Global*, (11), 5.
[270] Justice Chelameswar Opinion (pg. 12), Supra, 267, pg., 278.
[271] Ibid, pg. 277.

The majority opinion of Justice Chandrachud and the concurring opinion of Justice Kaul concretises the test for justification of the interference. Both opinions move closer to the European standard of proportionality that balances individual rights and state interests. Justice Chandrachud set out the three-fold requirement of:

> *(i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them.*[272]

Justice Chandrachud's opinion provides the grounds of justification for judicial purposes, which reflect the interdependencies of the Right to Privacy with other fundamental freedoms. The first test of *legality* emanates from the phrase 'procedure established by law', which means that there should be a law that justifies the infringement of Privacy. The second parameter of *necessity* requires the existence of a legitimate state aim. The test is grounded in Article 14 - Right to Equality - zone of reasonableness, which ensures that the nature and content of the law do not suffer from manifest arbitrariness. The third and last test of *proportionality* is an already existing test emanating from *PUCL*, which ensures that the state interference is proportional to the objective and purpose of the law.

In his concurring opinion, Justice Kaul also agreed with Justice Chandrachud's three-fold justification test; however, he added the fourth parameter of procedural safeguards against abuse of interference with rights.[273] As Justice Kaul explains, the fourth ground was needed to safeguard the rights of the individual in the current advanced digital age. Thus, the fourth ground echoes the similar need postulated in Article 21, a 'procedure established by law,' i.e., legislation need to protect a right by establishing safeguards. While advocating the need for law, Justice Kaul overlaps the first and the fourth ground. So, are there any procedural guarantees in India that safeguard the right to privacy against AI technologies? If yes, are they adequate, and aid courts necessity and proportionality analysis? Such questions are analysed in Chapter 6&7, we must return to how informational privacy needs to be evaluated.

[272] *Puttaswamy*, Supra 267, Part T, p., 264.
[273] Ibid, p., 533.

Puttaswamy provides us with the doctrinal foundation on which the Right to Privacy could be judicially tested, but it also holds that each privacy claim under Article 21 is contextual. An invasion of privacy must be evaluated and justified on a case-by-case basis. So, *Puttaswamy* settles the debate of a common ground for conceptualising privacy i.e., under the notions of life, liberty, and dignity, as mentioned under Article 21. But it leaves to the wisdom of the courts to conduct a necessity and proportionality test against the procedural guarantees stipulated by the legislature.

Though, the jurisprudential analysis allows us to locate the contours of right to privacy in India, to some extent, but it also raises the urge to establish a framework that aids examination of privacy in a context. As the above discussion of legal jurisprudence also shows, privacy claims are adjudicated based on public-private dichotomy or as a binary between disclosure and secrecy. Such boundaries are ineffective in privacy legal claims due to two reasons, a) The definition of what is public and private, and therefore what can be disclosed or remain secret keeps changing with time, across geographies and culture, and b) currently, the privacy legislations are framed to protect situations where privacy is expected and not where privacy is preferred. The above stated conceptualisations of privacy are also the result of such dichotomies and binaries. Thus, there is a need for a universal framework that allows adjudication of a right to privacy in settings that are complex, blurred (in terms of the public/private divide), and rooted in political and social contexts. This is because, privacy, specifically informational privacy, is violated in each context, due to the nature of the information involved, actors involved in transmitting information, the relationship between the data subject and the data controller and other variables in a context. The answer to a universal framework lies in Part C, which lays out Helen Nissenbaum's theory of contextual integrity that can aid our inquiry into Informational Privacy's determination.[274]

PART C: PRIVACY AS A CONTEXTUAL INTEGRITY

In *PUCL v. UOI*, the Indian apex court stated that "*as a concept, privacy may be too broad and moralistic to define it judicially …. whether the right to privacy can be claimed or has been infringed in each case would depend on the facts of a particular case*.[275] Helen Nissenbaum's theory of contextual integrity advances the said *PUCL* statement by demanding the study of a specific context within which the claim of privacy is being studied. Nissenbaum's theory is an informational privacy theory which argues that each context is constituted of informational norms, and when

[274] Helen Nissenbaum, Privacy as Contextual Integrity, 79 WASH. LAW REV. 119, 120–121 (2004).
[275] *PUCL v. UOI*, at page 311, pp. 18.

the norms get violated the right to privacy is said to be breached. The theory means that information gathering, and disclosure follow a particular context's governing norms. The central tenet of the said theory hinges on the understanding that everything in the world - inter alia our activities, conversations, expectations, transactions - occur in a context shaped by a distinct set of norms that govern one's actions, roles, and practices. Within these norms, the said theory focuses on the informational norms that govern the flow of information, in the sense of who collects the data, what type of data is collected, which the parties transacting is, and the practices within which such transaction of information is taking place. Thus, privacy depends on the informational norms entrenched in the 'characteristics of the background social situation'.[276] The chapter now deep-dives into two key parameters of the theory, i.e., a) Context and b) Norms.

3.1. Context

Nissenbaum, to define context, relies on the scholarly works of authors who have rigorously developed its meaning in social context theory and philosophy. Influential accounts in this field define social context as spheres of value,[277] a pattern of regularised conduct,[278] social fields,[279] cognitive structures,[280] social spheres,[281] and social orders.[282] Each context is shaped by certain activities, actors, internal values and norms, and standards across the vast array of meanings provided. Contexts are not formal constructs but rather abstractions of real-world representation. Defining context and itemising its characteristics is against its fluid character. Contexts are rooted in space, time, society, and culture, reflected in roles, activities, values, and norms. For example, a healthcare setting or an educational institution would be very different in India to that of the United Kingdom due to dissimilar disparities across the aspects of economy, history, culture, and politics. It is important to note herein that specific contexts within a given society are rigid and regulated by law or custom. For example, in a classroom setting, contexts like the dress code, start and end, and the state or private school actors regulate the time of the school or the exams.

---

[276] Nissenbaum, Supra note 274, p. 129.

[277] Talcott Parsons, Erving Goffman and Max Weber coined the term. For more details: Goffman, E. (1949). Presentation of self in everyday life. *American Journal of Sociology*, *55*, 6-7. Also see, Religious Rejections of the World and their Directions', in H. Gerth and C. Wright Mills (eds.), From Max Weber: Essays in Sociology (London: Routledge): 323-59.

[278] Martin, J.L. 2003. *What is Field Theory?* American Journal of Sociology 109(1): 1-49.

[279] Bourdieu, P. 1984. *Distinction: A Social Critique of the Judgement of Taste*. Richard Nic, trans. Cambridge, MA: Harvard University Press.

[280] Abelson, R., & Schank, R. C. (1977). Scripts, plans, goals and understanding. *An inquiry into human knowledge structures New Jersey*, *10*.

[281] Walzer, M. (1984). Walzer, Spheres of justice: a defence of pluralism and equality.

[282] Schatzki, T. R. (2001). *Practice Mind-ed Orders*," pp. 42-55 by Theodore R. Schatzki, Karin Knorr Cetina and Eike von Savigny. *The Practice Turn in Contemporary Theory*.

On the other hand, students' interaction, questions posed to the teachers, or how one sits in a class need to be specified. Thus, it should not be surprising that there might be many variations in the actors, norms, and values in a given setting. It is important to note such variations in a specific claim of right to privacy makes each case unique. There are several contexts and sub-contexts interrelated and sometimes interdependent. There can be an 'unregulated context' of peer-to-peer interaction in the earlier classroom example, but there is also a regulated sub-context wherein the class monitor can dictate certain acceptable practices while interacting with peers through school norms. Thus, contexts overlap and conflict with each other.

3.2. Norms

Nissenbaum provides an understanding of norms based on the existing scholarly work of authors in law, social sciences, philosophy and other allied fields. She notes the ambiguity in two kinds of norms: one which mandates or prescribes specific rules or codes of conduct to be performed, and others merely descriptive and refer to standard practices or behaviour with no expectation. Cristina Bicchieri terms the former as injunctive norms and the latter as descriptive norms.[283] Within the said framework, Nissenbaum uses the injunctive or prescriptive norm to overlap with the dominant interpretations in canonical works of H.L.A. Hart or Joseph Raz.[284] Nissenbaum adopts Raz's four critical elements of norms: a) a prescriptive '*ought*' element, b) norm subject - upon whom the obligation of the norm falls, c) norm act - action prescribed in the norm and d) condition of application - the context in which the norm act will be obliged by the norm subject.[285]

Nissenbaum highlights that just like the variation in contexts, the norms also experience variability in at least two dimensions: a) the degree to which norms are expressed and b) norm type. The first variation considers whether a particular norm is explicitly expressed, followed, and sanctioned by authoritative individuals and institutions or implicitly accepted in the context. The second dimension categorises the norms according to their nature of prescription, example, moral norms, which can be concerning social conventions of etiquette like not interrupting others while talking or any act of stealing, physical harm, and others. Others can be religious norms, historical norms

[283] Bicchieri, C. (2000). Words and deeds: A focus theory of norms. In *Rationality, rules, and Structure* (pp. 153-184). Springer, Dordrecht.
[284] Raz, J. (1999). *Practical reason and norms*. OUP Oxford, p. 50.
[285] Nissenbaum, Supra note 274, 139.

based on custom or usage, and legal norms. Thus, a context assembles norms that govern the actors and their underlying activities and practices.

For our discussion in this thesis around informational Privacy, Nissenbaum's norms governing the flow of information should be focused upon in a particular context. She terms such norms as informational norms that comprise of a) Context, b) Actors, c) Attributes and d) Transmission principles. While Context is discussed above, the other three parameters are now discussed in the next sub-section with an expectation that they would aid in the formulation of a framework to conduct context-based determination for a privacy claim, which *Puttaswamy* judgement recommends.

CONTEXT RELATIVE INFORMATIONAL NORMS

3.3. Actors

Informational norms characterise three critical actors: the sender of the information, the informational receiver, and the information subjects. In many cases, Nissenbaum recognises that the sender and the subject might be the same individual or organisation.[286] She states that to specify an informational norm, the actor's contextual roles are essential to examine and understand. For example, in a school setting, there are numerous explicit and implicit informational norms prescribing the sharing of data on the subject (child) between the sender (students) and receiver (teachers, principals). The context-relative informational norm will change if the sender(s) are the school authorities, and the receiver is the third party contracted by the school for services. Thus, discussion of the actors and their role in each context is crucial to highlighting variability in informational norms relevant to privacy.

Nissenbaum states that '*the capacities in which actors' function are crucial to the moral legitimacy of certain information flows*'.[287] It is true as it is the individual's choice to provide limited access to its information to some actors, based on the degree of appropriateness. While the limited access norm is not always explicit and might depend upon the relationship with another actor, like husband-wife, there is a need for a norm regulating the flow of information in other relationships, especially where there is a possibility of information asymmetries like doctor-patient, student-

[286] Nissenbaum, Supra 274, p. 141.
[287] Ibid, p. 142.

teacher, and others. Thus, the theory of contextual integrity enhances the possibility of innumerable actors and their underlying capacities and relationships.

3.4. Attributes/Information Types

The following parameter shifts the focus from whom and to whom the information was shared to an equally important question of the information shared. Nissenbaum terms it as *attributes* denoting the nature and information type integral to defining the informational norms. Again, taking the school context, all kinds of information - Name, Bank account number, payment details, health details, insurance carrier, learning data, course data, and assignments - are collected, aggregated, and disseminated. Contextual integrity does not typify the attributes along the public-private or personal-non-personal divide; instead recognises an array of possibilities. Informational norms might render a collection of specific attributes of the subject as appropriate, for example, the course data (courses in which the student has enrolled, course settings, submissions of assignments) but others as inappropriate or with caveats like the personally identifiable data.

Some authors have divided the appropriateness of sharing attributes into binaries. For instance, Charles Fried categorises attributes as less intimate and more intimate, i.e., more minor intimate attributes can be shared with the larger society and more personal attributes to closer sets of family and friends. However, such dichotomy suffers from not considering context as sharing attributes varies over time and space. In certain cultures, sharing the age of the female is considered sensitive, personally identifiable information. Alternatively, in some religions, women are expected to be *pardanashin i.e., hidden behind a veil or a screen*. Thus, the factors defining a particular attribute are variable, proving the inadequacy of defining. Though providing a finite taxonomy of applicable attributes in circumscribed narrower contexts is possible, it might be a useless exercise in an evolving context and co-evolving institutions, roles, actors, and practices.

3.5. Transmission Principles

The last parameter of context-relative informational norms stipulates the terms and conditions shared between the required actors. It can be co-related to Raz's first element of the norm - 'ought element' - i.e., the conditions under which information ought to be (or not) shared. There are infinite principles embedded in informational norms, like consent (gathering or disseminating information only after seeking permission from the sender/subject), notice (providing knowledge to the subject), or confidentiality. Such principles work in sync with the other parameters of the framework.

The transmission principles, a sub-part of informational norms, can provide the basis for (or negate) the actor's conduct and shared attributes. Drawing from the familiar experiences of the school setting, information regarding the school grades is often between the student and the teacher due to the principle of reciprocity. However, in specific contexts in a school, the reciprocity principle is overruled due to the unidirectional flow of information, like when a teacher imparts knowledge in a lecture. A difference occurs when rules or codes of conduct dictate a particular flow of information. For example, during the admission process, a child is mandated to put forth their health conditions, disabilities, religion, and other personally identifiable details to aid the school in making improved choices.

Thus, the theory of contextual integrity provides a conceptual framework to discuss and examine Right to Privacy, which could apply to varying contexts spread across cultures, historical periods, and places. It also punctures the dichotomy of the public-private divide through which the Right to Privacy is generally analysed and regulated. Rather than focusing on specific conceptualisations of informational privacy breaches like disclosure or inability to control information, the contextual integrity framework shifts our focus to several variables, the function of which determines whether an individual's informational privacy is violated in a context or not. The framework provides the contours to adjudicate the claim to informational Privacy which is now applied to the Indian schools in the next chapter, wherein also lies the thesis' novelty.

CONCLUSION

The attempts to locate one common conceptualisation of privacy proved to be an unsatisfying exercise. However, it gave us an indication to examine a privacy claim differently. Part A begins with examining and critiquing existing dimensions of privacy while questioning whether there exists a common denominator of privacy. It concludes that though there is a vast array of scholarly literature on justifying the meaning of privacy, it either broadens or narrows privacy's conception to a public-private dichotomy.

Part B focuses on informational privacy, proving through various judgements by the Indian Supreme Court that the phrase encompasses all the conceptions of privacy discussed in Part A. Part B deep dives into formulating informational Privacy in India, though it does not provide a specific conceptualisation. For instance, *MP Sharma* and *Kharak* conceptualise it as the '*Right to be let alone*' in providing guidelines around search and seizure. *Gobind* and *Malak* carried forward

such conceptualisation of informational Privacy and permitted targeted surveillance under certain conditions, therefore treating informational Privacy as not absolute. *PUCL* extended the said conceptualisation by stating that telephone conversations are '*intimate*' to the individuals partaking, and they would not want the conversations to be published to the world, holding their '*secretive*' nature. The post-*PUCL* development clarified the third-party doctrine through *Canara* by laying out norms for the flow of personal information. Thus, Part B shows that there are several contexts, like marriage, procreation, family and privileged relationships, child rearing, telephonic communications, banking, education, thoughts, tastes, preferences, et.al. where a claim of informational privacy can take multiple shapes and forms. It indicates that the privacy claim is fluid and should be judged on a case-to-case determination. Part A and B's discussion provide common constituents of privacy but raise questions around its adjudication in different contexts. Thus, both parts leave the reader with the question that conceptualising privacy is unsatisfying but provides certain common denominators seen in an informational or decisional privacy claim like disclosure, control over information, secrecy, limited access etc. But would not defining privacy open the floodgates for the judiciary to embark on separate journeys while adjudicating privacy claims?

Part C opens by justifying why Helen Nissenbaum's theory of contextual integrity helps provide the contours of an informational privacy framework that the courts can incorporate in their adjudication and legislature can use to frame the pillars of a data protection legislation. The usefulness of this framework lies in not generalising the concept of privacy but instead appreciating its breadth in particular '*contexts*'. While presenting it as a contextual problem, it shifts the homogeneous question of conceptualisation, as certain concepts are too fluid to be defined. To appreciate privacy's plurality, the framework provides us with four key parameters, essential in the digital age, laying out the direction for future researchers to recognise the '*contexts*', dissect the '*actors*' and the '*attributes*' in each context, understand the '*transmission principles*' on which a set of practices are being performed. The goal of the theory is to produce '*informational norms*' after studying the context, actors, and attributes, useful to regulate privacy in a given context. Thus, the understanding of context relative informational norms would aid the development of a legislative framework by the end of the thesis.

The next chapter applies Nissenbaum's contextual integrity framework to an Indian school setting. It adds uniqueness to the existing literature in terms of blending technological systems and the social context of an Indian school to dissect the sites of privacy claims. For such purposes, the

next chapter embarks on interdisciplinary research to first, explain the '*context*' of an Indian school, how it operates on an everyday basis, and second, the '*actors*' who collect, share, and store '*information types*' leading to breach of children's right to privacy. The next chapter will show that children's right to privacy is rooted in the school's social and political context, shaped continuously by the actors at play and the motivations of such actors behind information flows, aiding courts, and legislature's understanding of a privacy claim.

FOURTH CHAPTER

CONTEXTUAL SETTING OF AN INDIAN SCHOOL

Social Institutions like schools aim to impart knowledge based on a predefined curriculum. Schools also serve the purpose of aiding social interactions that enable the formation of an identity of an individual. They instill life skills like autonomy and agency, i.e., control over decisions and power to decide. However, digital technologies like CCTV cameras, fingerprint scanners, facial recognition software, etc., that are pervading schools in India end up weakening such essential features of 'personhood' that constitute the right to privacy.[288] In 2020, COVID further accelerated the installation of such systems where thermal scanners, emotion recognition systems, and facial recognition cameras meant for proctoring became part of the necessary school infrastructure, taking the panopticon outside of the school premises into the private space of students.

Technology in the education sector has shifted from merely enabling or assisting educational learning to predicting, controlling, and restraining the children within the enclosed spaces of a school's territory. Before understanding the scope and extent of AI-based surveillance technologies in schools and how they breach children's individual privacy rights, it would be crucial to understand the interaction and experiences of students, teachers, and other staff members with these technologies. Though each interaction is subjective, it would provide a roadmap of the 'context' within which such technologies operate and how they navigate the relationship between students and student-teachers. The theory of contextual integrity enables questioning of the domination, information asymmetry, unaccountability, opaqueness, control and exploitation by a given technology.

Digital Sociology is a theory that enables the reconfiguration and reorientation of a space in conjunction with digital technologies. It is a theory that has come to grips with the ever-changing technological landscape and studies how societies shape digital technologies and vice-versa. The said theory challenges the idea of technological determinism and acknowledges both the '*materiality*' of technology and the '*practices*' that shape societies.[289] The '*practices*' analyse the

[288] Raab, C., & Goold, B. (2011). Protecting Information Privacy, Equality and Human Rights Commission Research Report 69.
[289] Fussey, P., & Roth, S. (2020). Digitising sociology: Continuity and change in the internet era. *Sociology*, *54*(4), 659-674.

social relationships, everyday engagements of people with technology and the formed identities by way of technology, i.e., the contextual setting within which the technology is situated. Herein, 'practices' can be associated with Nissenbaum's theory of privacy as contextual integrity (as discussed in the last chapter), which defines context as a space rooted in societal values and culture, reflected through activities and norms shaping the setting. Thus, Helen Nissenbaum's theory is a subset of broader digital sociology theory that aids our understanding of technologies by studying the settings in which technology is designed, developed and deployed.

Part A of this chapter lays out the contextual setting of an Indian school, where a technology is deployed, by examining the daily '*practices*' through which a child produces its identity. Part A brings examples of emerging technologies and cuts through the axes of social settings to show how they (re)shape an individual's identity. The practices aspect of technology is sociological and steers its way through the expressions, identities, and culture of an individual that technology shapes. Thus, digital sociology produces a sociological view of technology that cultivates its associations with power, information asymmetry, discrimination, and freedom to make decisions, the features constituting informational and decisional privacy. Part A brings forward the social and political context of an India school where the thesis is trying to argue for safeguarding the informational privacy of students.

Each context also includes the actors connected to the information flows who are responsible for collecting and processing various attributes/information types. Foucault's notion of '*neoliberal governmentality*' examines the market forces or other actors advocating and promoting techno-surveillance devices in schools. It is maintained that market forces have the potential to shape the political decisions and motives of the state to push the deployment of surveillance technologies in schools.[290] For said reasons, **PART B** of this chapter shows how citizens' and states' dyadic relationship is seeing a shift in the age of surveillance due to the inclusion of new stakeholders, precisely the market forces, making it a triadic relationship. Exploring this triadic collaboration and situating the fundamental rights amidst the actor's incentives is necessary. This is because the different incentives and motivations drive the collection, sharing and processing of personal data in schools. Such incentives ignore the contextual settings, i.e., everyday life practices in a school. Part B shows how the triadic relationship of the state-citizen-market aids the creation of a technological architecture - the '*education stack*' - a centralised repository of all

[290] Kasinathan, G. (2020). Making AI work in Indian education. *Artificial Intelligence in India*, *6*.

student education records breaching the security and privacy of students in schools. This is evaluated through the impact of the triadic relationship in the fortification of schools by justifying a culture of data extractivism where refusal to share data leads to exclusion. **PART B** uses the case study of Aadhaar - a central government scheme - to show the triadic relationship that is further linked to several state-level schemes, enabling the building of an education stack. Thus, Aadhaar further elucidates Helen Nissenbaum's theory by laying out the actors and attributes involved in a school context.

The novelty of this chapter lies in considering the digital sociology theory in further deciphering the contextual setting of a school by laying out the formed relationships, shaped identities, and the resulting knowledge. Part B of the chapter uses the case study of Aadhaar to showcase how data aggregation of the knowledge produced at school with the Aadhaar database makes an individual completely visible. The application of digital sociology sits well with examining the right to privacy in a school, as privacy is both an individual right and a societal right as it protects different forms of social interactions. It is shown that individual privacy is important to be safeguarded in schools to preserve the sanctity of the relationships of a school (student-student, student-teacher) and the school's democratic functioning. In the context of the nation-state, *Ruth Gavison* notes a similar point, "*Privacy is essential to democratic government because it fosters and encourages the moral autonomy of the citizen, a central requirement of democracy*".[291] When placed in a school, technology mediates through the axes of different subjectivities and shapes students' identities and social relationships. Thus, a particular technology fits into an institutionalised setting mediating its social relationships, governing the flow of knowledge/data and thus regulating children's informational and decisional privacy.

PART A - CONTEXTUAL SETTING OF AN INDIAN SCHOOL SYSTEM

India's education regime is highly differentiated, unequal, and stratified. It can be understood from the nine types of schools functioning in India that align with the socio-economic classes from which a particular student belongs.[292] The types of school do not provide the variety for the parents

[291] Gavison, R. (1980). Privacy and the Limits of Law. *The Yale law journal*, *89*(3), 421-471.
[292] The nine type of schools include: **(i)** Ashramshalas (for Adivasi/tribal regions); **(ii)** state-run government schools (including municipal, corporation and panchayat schools); **(iii)** state-aided but privately managed schools; **(iv)** centrally aided special schools such as the Kendriya Vidyalayas, Navodaya Vidyalayas and "Military Schools"; **(v)** low-fee paying, state-syllabus private schools; **(vi)** expensive private schools including the "Public School" chains; **(vii)** religious schools (Pathshalas and Madrassas run by religious institutions and trusts); **(viii)** alternative schools run by independent or non-profit organisations; and **(ix)** international schools.

to choose for their students, rather, the government enrolment data gives away that the lower caste, lower class, or low economic background people opt for government schools.[293] Such students can also study in English-speaking international schools or private schools, based on government reservation or state sponsored funding.[294] Thus, there is a constant differentiation between students on the grounds of caste, class, sexual orientation, economic background and others that ruptures the basic ethos of social relations and identities. It is in this chaotic space technology is introduced to further capture students' identities that they might not want to bring to the surface. Thus, as this chapter will show, technologies overlook the socio-economic context of the school and are designed, developed and deployed to create a panopticon within a school that has both direct and disparate impacts on students' privacy. Thus, understanding the social structures by setting out the 'context' and their interaction with educational technology would help understand and evaluate the nature of the breach of privacy rights.

1.1. Representation and Composition

Schools as institutions are a perfect destination for institutional discrimination and labelling based on heuristics, biases and stigmas attached. Conceptions of stigma, outlined by *Erving Goffman*, typify instances in which an individual in a school might feel stigmatised:

> *"First, there are abominations of the body -the various physical deformities. Next, there are character blemishes like a weak will, unnatural passions, dishonesty, and treacherous and rigid beliefs inferred from a 'record' of mental disorder, homosexuality, suicidal attempts, radical political behaviour, or addiction. Finally, there are stigmas attached to race, religion, and nation which can be transmitted through lineages and contaminate all family members".*[295]

Discrimination and biases in India arise from ancient notions of Veda (religion) and Varna (caste). According to the predominant Hindu religion in India, society is classified into 4 Varnas: Brahmin (priest), Kshatriya (Warriors), Vaishyas (traders) & Shudras (Servant). They are further subdivided into smaller castes, with Dalits (untouchables) and Scheduled Tribes outside the caste system. By having surnames, one can denote which religion and caste the person belongs to. Thus, stigmatisation based on caste is an everyday part of Indian social life. For instance, a vast body

[293] Vasavi, AR, School differentiation in India reinforces social inequalities, The India Forum, April 12, 2019, Available at https://www.theindiaforum.in/article/school-differentiation-india-reinforcing-inequalities.
[294] Ibid.
[295] Goffman, Erving. *Stigma: Notes on the management of spoiled identity*. Simon and Schuster, 2009.

of empirical literature proves that a higher caste leads to impeccable educational attainment and chances of growth.[296] A study by the University of Maryland and the National Council of Applied Economic Research (NCAER) also shows a disparity in student enrollment and drop-out rate based on caste and religion.[297]

When a technology is introduced amidst such historical discrimination it paves the way for historical bias - reinforcing the stereotype of the world as it is. For example, in the context of this thesis, AI technology used to predict the dropout rate of students trained on historically biased caste or gendered datasets will reinforce harmful stereotypes against girls or children belonging to lower castes or marginalised populations. Similarly, live facial recognition technology systems (LFRT) meant to provide security or discipline is ineffective in capturing the historical biases that cause indiscipline in the first place. As an anonymous interview shows, a Dalit student was outed by upper caste teachers and students by hurling casteist abuses and slurs.[298] Such indiscipline or conversations, even if captured by LFRT systems, would potentially be considered normal due to the stratified society in which such conversations occur. A study by *Mohammad Talib* has also shown the contemptuous attitude of upper-class teachers towards students either belonging to lower castes, classes, religion, or from a poor social and economic background.[299] This leads to marginalisation, disengagement, and sometimes, resistance to a teacher from an upper-class background. When humans are themselves implicitly and explicitly biased, it is dangerous to presume that the installation of AI systems would not stealthily include the same biases. Thus, every day, the language of discipline, hard work, ability, and social relationship is shaped by class, gender, caste, and other social factors.[300]

Historical biases pervading discrimination do not self-evidently breach students' privacy rights. But AI technologies, like one predicting dropout, do not allow students to find out what information

[296] Desai, Sonalde, and Veena Kulkarni. "Changing educational inequalities in India in the context of affirmative action." *Demography* 45, no. 2 (2008): 245-270. See also, Anitha, Bhaskara Kurup. *Village, caste and education*. Rawat Publications, 2000.
[297] Sonalde, Desai, D. Adams Cecily, and Dubey Amaresh. "Segmented Schooling: Inequalities in Primary Education." (2009): 230-52.
[298] Naraharisetty Rohitha, “Casteism still thrives in elite schools in India. What would Anti-Caste Education Look Like?”, Swaddle, July 14, 2021. Available at https://theswaddle.com/casteism-still-thrives-in-elite-schools-in-india-what-would-anti-caste-education-look-like/.
[299] Talib, Mohammad. "Ideology, curriculum and class construction: observations from a school in a working-class settlement in Delhi." *Sociological Bulletin* 41, no. 1-2 (1992): 81-95.
[300] Thapliyal, N. (2012). Unacknowledged rights and unmet obligations: An analysis of the 2009 Indian Right to Education Act. *Asia-Pac. J. on Hum. Rts. & L.*, *13*, 65.

has led the technology to classify them in categories. While categorisation/profiling of students on any protected characteristic directly leads to discrimination, it also causes vulnerability, discomfort, and uncertainty in the student's mind. Such forms of insecurity can lead to powerlessness and control concerning personal information. Thus, it is pertinent to note that historical biases due to caste, class, gender any other characteristics can, in the context of AI technology: *1)* Affect students' emotions leading to under-achievement, *2)* Exacerbates surveillance, inequity, impartiality, and digital divide as individuals collecting and processing data are themselves biased. The Information Commissioner Office notes in its Taxonomy of Harms, technologies purposefully causing emotional distress, detriment to mental health or loss of confidence need regulation.[301] Technology's interaction with a stratified society has the potential to overlook society's representation and composition, leading to the simplification of its predictions, stigmatising and interfering with the most intimate aspects of identity, i.e., the self.

1.2. Identity Formation

Character and identity of 'self' are not built in isolation but through reflective engagement with the environment. Learning and the teaching environment can shape a child's school conversations, attitudes, and behaviour. Concerning this, the work of *George Herbert Mead* is influential as he distinguished between the "me" and "I".[302] *Mead* explains that "Me" is what the personal self wants to see, but "I" consists of characteristics and attributes which have metamorphosed over time. Thus, example, in a kindergarten, a student's "me" would constantly move around a class, but when the teacher scolds or guides a student's behaviour, it becomes their "I". Thus, the attitude of the teacher fosters a reflective engagement in a student that is reworked, rethought by the student, and becomes part of its "Me" - both "Me" and "I" contributing towards the development of 'self'. This is called a symbolic interactionist perspective in which the surrounding environment, like the presence of teachers, parents, or factors like patriarchy, caste, religious festival celebrations, and attitudinal behaviour towards the disabled, forms part of the everyday reality of a school and shapes a student intrinsically.

While a symbolic interactionist perspective looks mainly at an individual's reflective engagement, another school of thought, dramaturgical sociology, looks at the interactions between people.

[301] Overview of Data Protection Harms and the ICO's Taxonomy, Information Commissioner Office, April 2022, Available at https://ico.org.uk/media/about-the-ico/documents/4020144/overview-of-data-protection-harms-and-the-ico-taxonomy-v1-202204.pdf.
[302] Mead, George Herbert. "Mind." *Self, and Society from the Standpoint of a Social Behaviorist.: University of Chicago Press: Chicago* (1934).

Erving Goffman argues that specific social interactions are short and henceforth cannot impact the 'self'. However, routine interactions create a set of 'fronts', 'expressions', and 'ways of self-being that seem acceptable in a given setting. For example, a student is said to be attentive if taking notes, answering questions, or expressing attentively. However, in the guise of taking notes, a student might be drawing or playing something. So, how would an AI-based proctoring technology detecting the emotions of a student perform in such cases?

Meenakshi Thapan's book, *Life at School,* applies both Mead's symbolic interactionist and Goffman's dramaturgical sociology perspectives in Indian schools.[303] She discusses the organisational structure and reflective engagements in *Rishi Valley School* to show the presentation of the 'self' and, simultaneously, negotiation during encounters. Teachers deploy various teaching styles - the lion tamer, the entertainer and the romantic[304] - to exert a sense of power over students to instruct and engage them, to bring discipline in the class, supposed to increase student engagement. However, simultaneously, students are involved in a continuous negotiation, resistance, and struggle to maintain their autonomy. Thus, *Thapan* shows that classrooms are a site of constant presentation of the self, negotiations and maintaining personhood.

Mead finds relevance in the digital sociology of school architecture as he shows that confidence, shyness, participation levels in the class, and introvert-extrovert are characteristics of students which change due to interaction with the environment. Thus, in Mead or Goffmanesque's view, it can be inferred that digital technology is also part of the classroom environment that mediates through different student characteristics invoking changed reactions, i.e., 'I' transforming into 'Me'. FRT systems meant for proctoring or gauging a student's attentiveness level in a class can yield incorrect predictions, as students' behaviour will metamorphose with the technology in play. Thereby the incorrect predictions of the child being not attentive in a class or cheating during an exam might lead to wrongful sanctions/punishments.

Another technology, namely, Facial Recognition embedded CCTV cameras, when mediated along the axes of caste, class, or gender, has the potential to create a culture of fear and repression. Certain protected characteristics, like being from marginalised communities like Dalit, Muslim, Scheduled Tribe or having homosexual attributes, have attracted punishment, and have

[303] Thapan, Meenakshi. *Life at school: An ethnographic study*. Oxford university press, 2006.
[304] Hargreaves, David H. *Interpersonal relations, and education*. Routledge, 2017.

also led to death.[305] The societal fear and the knowledge of being recorded in a class creates psychological harm that leads to curbing decisional privacy and censorship. Students' identities formed within such psychological fear violate their integrity and dignity - two essential facets of the right to privacy.[306]

1.3. Peer Culture

Peer culture is a significant part of school practices and can also be analysed through Mead's or Goffman's theory. The culture of forming relationships is not merely an identity formation exercise and henceforth demands separate attention. It is an informal culture absorbed and contrasted with a disciplined, routinised aspect of schooling (curriculum, timetable, calendar), which enables a sense of belonging and forms an identity but also provides entertainment. Anuradha Sharma, in her ethnographic study conducted in a Delhi school, states that relationships between students are essentially an informal space outside the scope of school authorities where they have their own rules of '*interaction*' and '*membership*'.[307] Sharma's fieldwork demonstrates the existence and significance of these relationships on the pretext of '*Help*' & '*Fun*' - the two main recurring themes for having peers in schools.

Sharma's study is unique as it notes the context in which there can be rifts in these relationships. These rifts largely depend upon age, gender, stereotypical imagery, a mental fight between traditionalist and modern values, and many other factors outside the school's scope to resolve. As children turn into adolescents, the study finds the stereotypical segregation of boys largely having no friendships with girls and vice-versa. Also, in a gendered context, this theory notes the communicative style of each group, with girls depicting helpfulness and life-long trust and boys as peers valuing trust but showing a carefree, fun attitude validating *Carol Gilligan's* comment of "*dependent femininity and independent masculinity as distinct moralities for the two genders"*.[308]

---

[305] Kumar, Mayank, The Hindu, Sept 26, 2022, Available at, https://www.thehindu.com/news/national/other-states/dalit-student-dies-after-being-beaten-by-teacher-opposition-mounts-pressure-on-government-for-action/article65937441.ece.

[306] Bloustein, E. J. (1964). Privacy as an aspect of human dignity: An answer to Dean Prosser. *NYUL rev.*, *39*, 962.

[307] Sharma, Anuradha. "Negotiating school and gender: Peer performatives." *Ethnographies of schooling in contemporary India* (2014): 21-65.

[308] Gilligan, Carol. *In a different voice: Psychological theory and women's development*. Harvard University Press, 1993. Though it is a deeply contested aspect of feminist thought but the statement in the thesis context tries to establish that surveillance operate differently on different genders.

With technology at every corner of the school, monitoring students' every movement runs the risk of breaching the zone of privacy that an intimate conversation requires. The government of Delhi and the public works department intends to share live footage of CCTV cameras with the parents/guardian of their children. A pilot project for implementing such a scheme has already been done at fifty government schools in Delhi.[309] Though the government depicts a narrative of care, security, and discipline behind introducing such measures, it simultaneously ignores the parental and school 'control' that arises. With a tracking device over a student's head, knowing that talking to a girl, Muslim, or a homosexual peer would be knowable to the parents potentially changes the communication and negotiation patterns of a child in the 'zone of surveillance'. Without a tracking device, the child would have continued normal encounters and interactions without subjecting them to caste, gender, class, or sexual orientation. Children's interactions with technology continuously forge new notions of peer relationships and their individual identity in a school.[310]

1.4. Mode of Assessments

Educational assessments are meant for individual growth and social change.[311] However, if conducted disproportionately, they can lead to social exclusion. Schools relying only on the final examinations reinforce social inequalities and create a merit-failure gap within a school. So, Indian schools follow multiple assessment forms, like one like the United Kingdom, a mixture of classroom assessments (formative) and final/end-of-the-year assessments. The difference between the mode of assessment is that even classroom assessments contribute to the final grading. School assessment systems, though consisting of a formative and summative assessment, are managed by different boards - Central Board of Secondary Education, ICSE, State Boards, IB, NIOS, etc. For a student who wishes to change the board for senior secondary education (A Levels) from the one it had during secondary education, there is a cultural shift in terms of the medium of instruction, methods of teaching and assessment, focus areas, and level of teacher training. The new National Education Policy (NEP, 2020) considers the concerns associated with different education boards, teacher practices, and assessment styles.[312] The NEP

[309] Jain, Anushka, *Hey CM, Leave these Kids alone*, Internet Freedom foundation, 30th July 2022, Available at, https://internetfreedom.in/hey-cm-leave-those-kids-alone/.
[310] Rooney, T. (2012). Childhood spaces in a changing world: Exploring the intersection between children and new surveillance technologies. *Global Studies of Childhood*, *2*(4), 331-342.
[311] Boli, John, F. Ramirez, and J. Meyer. "Explaining the origins and expansion of mass education." *Sociological worlds: Comparative and historical readings on society* (2000): 346-354.
[312] National Education Policy, 2020, Available at https://www.education.gov.in/sites/upload_files/mhrd/files/NEP_Final_English_0.pdf, pg. 60.

2020, framed by the Ministry of Education, Government of India, intends to integrate technology with Online assessments and examinations. The policy proposes the establishment of bodies like the National Assessment Centre (NAC), school boards, and National Testing Agency to implement assessment frameworks encompassing the design of standardised assessments, assessment analytics, competencies, etc. However, the policy document lacks the meaning of '*standardised assessment*', without which there is a possibility of an imbalance of power in favour of the elite and privileged, establishing an exclusionary nature of school practices.

In terms of assessment, there are subtle cues, words, language, context, and sentence formation which a teacher evaluates.[313] Such factors are subjective and raise the question of their inclusion in an AI system model. In India, assessments also include weightage of class behaviour and the student's punctuality in terms of attendance, homework completion, and class participation. In the broader socio-cultural Indian society, class participation cannot be a valid means of assessing a child. This is again because of its subjectivity, example, in India, disagreeing with elders is considered a moral wrong and invites punishment. Classroom participation can have varied meetings, from giving correct answers, raising questions, or simply agreeing to the teacher's instructions. Thus, the teacher-student dynamics should be seen in an ethical interactionist setting where students answer correctly or keep quiet. In such a setting, *Krishna Kumar* states that '*Adivasis/Scheduled Tribes*' prefer not to "*question or quibble*" with the "*imposing figure of the teacher*".[314]

The subjectivity with which a teacher assesses a child is difficult to capture and replicate through AI technology. A push towards using AI technologies for assessment ignores the fluidity of the above-said factors and considers a uniform assessment. To test 'higher order skills like critical thinking, competency-based learning, and conceptual clarity requires a holistic development and overhaul of the current school education system. Thus, AI systems deployed by private or public schools to assess student ignores the cultural processes ingrained in the Indian education system and create exclusion.

[313] Payne, George CF. "Making a lesson happen: An ethnomethodological analysis." The process of schooling: A sociological reader (1976): 33-40.
[314] Kumar, Krishna. *Social Character of Learning*. SAGE Publications India Pvt. Ltd., 1989.

1.5. Teaching Methods

Various states in India are installing CCTV cameras in government schools, community schools and madrasas - specifically classrooms, for the due diligence of students and teachers. For example, the '*Gunotsav scheme*' of Gujarat came in 2009 and is considered the brainchild of the current Prime Minister of India, Narendra Modi, who was then the state's chief minister.[315] Under the scheme, the state government officials get first-hand information about each student and teacher in their state through surprise interactions or by daily monitoring done through Information Technology tools.

The influx of digital monitoring tools does not ensure the construction of knowledge by the teachers in the classroom. The cultural pedagogy in India focuses on rote learning and subjective assessments, thus, demanding no shift from the current teaching techniques.[316] Nevertheless, several policy documents like the National Curriculum Framework,[317] National Council for Teacher's Education Curriculum Framework for Teacher Education,[318] and the recent Niti Aayog's AI strategy,[319] which notes the rote-learning and non-interactive nature of school practices, suggest solutions like Artificial Intelligence.

Rather than teacher and student surveillance, there needs to be transparency and accountability mechanisms to improve teaching methods. A sociological evaluation of a classroom needs to be done to design such mechanisms. The majority of schools in India do not follow a Socratic method of teaching where students attend classes to discuss, counter-question the teacher, solve their doubts, and do their readings for each class. In contrast, students attend or are presumed to attend the class as a blank slate and act on the mechanical direction of teachers who follow defined procedures and fixed knowledge. *Gaysu R Arvind's* study of Government and community schools in Rajasthan shows the mode of teaching subjects like Maths where memorisation of the

[315] Department of School Education & Literacy, Ministry of Human Resource Development, Government of India, "Detailed Assessment Report (NGOs and Private Organisations), 2011, available at https://www.education.gov.in/en/sites/upload_files/mhrd/files/upload_document/Annexure%20II.pdf."
[316] Mili. "Pedagogical reform in Indian school education: Examining the child-centred approach." *Journal of Philosophy of Education* 52, no. 3 (2018): 533-547.
[317] National Council of Educational Research and Training, National Curriculum Framework, New Delhi, NCERT, 2005.
[318] National Council for Teacher Education, National Curriculum Framework for Teacher Education, New Delhi, NCTE, 2009.
[319] Infra. Note 324, pg. 35.

problem question is the strategy rather than outlining the conceptual rationale.[320] The '*teacher's method*' prevails rather than a student and teacher's co-constructive participation and negotiation. Another study by *Lakshmi Bhatia* in the schools of Mizoram also shows the hierarchical and didactic attitude of teachers exercising power and coercion upon students.[321] Her research also noted that, especially in rural schools, a whole lot of energy was spent by teachers in controlling and disciplining the students, which led students to disengage and pay token attention in the classroom. Thus, pedagogy is an important criterion that alienates students from what is being taught in the classroom and causes them to drop out of school.

Thus, upon laying out what *Helen Nissenbaum* terms as '*context*', it is learnt that the state, rather than developing a holistic policy around improving the skills of teachers through government schemes, believes in: a) harnessing personal information of a student while overlooking the context, b) designing the technology with private partners based on the limited information collected, c) and then believing on the technology's predictions that are discriminatory as they are based on the limited data collected. Third-party private organisations access such personal data, and constant monitoring is done via a central command and control centre. Such centres eventually become centralised sites where the entire knowledge produced from a particular school is stored. Such centralised repositories hold vast troves of personal records and resemble like what *Haggerty and Ericsson* call surveillance assemblages.[322] In any privacy claim such contexts needs to be understood by the courts as this is where incorrect data is collected and feeded into a technology. Such incorrect data feeds biases into technologies predictions/judgements and is done without any consent practices. The next section of this chapter moves to the second principle of Nissenbaum's privacy as a contextual integrity theory, i.e., 'Actors'. It will examine the stakeholders in the 'context' of shaping an individual's privacy boundaries. The said examination is a crucial step to attribute liability in cases of breach of privacy rights.

---

[320] Arvind, Gaysu R. "Institutional context, classroom discourse and children's thinking: pedagogy re-examined." *Psicologia & Sociedade* 20, no. 3 (2008): 378-390. For more: a similar study has been undertaken by Padman Sarangapani, where she does an ethnographic analysis of a primary school in Delhi to see what goes into the process of disseminating knowledge by teachers and what are the characteristics of students as '*knowers*': Sarangapani, Padma M. *Constructing school knowledge: An ethnography of learning in an Indian village*. Sage Publications Pvt. Ltd, 2003, Jayaram, Indira. (2010). Understanding Science Teachers' Praxis: An Ethnographic Study of Science Teaching in Four Bangalore, Schools. Doctoral Thesis, National Institute of Advanced Studies.

[321] Bhatia, Lakshmi. *Education and society in a changing Mizoram: The practice of pedagogy*. Vol. 1. Routledge, 2010.

[322] Supra, Second Chapter, Part B, note 94.

PART B - ACTORS AND INFORMATION TYPES IN AN INDIAN SCHOOL CONTEXT

The abovesaid practices in an Indian school contribute to the construction of knowledge in each student. Discussing the rich body of sociological work done in this domain and evaluating its interaction with AI laid out the contextual setting in a temporal sense. The aggregation of school knowledge and its management, which refers to the daily collection, identification, and construction of each knowledge transaction between students, happens in the contextual setting described above. The low cost of computing power and the influx of e-learning platforms allow the collection of insurmountable personal data of students to provide customised learning solutions.[323] It encompasses effective data (behavioural data), personal identifiers, learning outcomes of each student, etc. to identify, sort, and then provide actionable models for school authorities to act, direct or provide guidance to students. An idea of building data architectures in schools aligns with what the Indian government's policy think tank, *Niti Aayog*, calls in its Artificial Intelligence Strategy 2018 - an '*Education Stack*'.[324] The strategy notes that AI cannot replace the teacher entirely; it can still assist teachers and efficiently and effectively manage classrooms, evaluate students' learning outcomes, develop customised educational curricula and personalise content and provide real-time feedback on student performance.[325] However, in a country where the majority of boards and the underlying teachers follow a pattern of rote learning, pre-fixed curriculum and pedagogy, and subjective assessments to gauge students' learning, there is a need for a greater emphasis on teacher training, development of new modules, and framing of ways of teaching rather than leaving it to AI technology to provide desired outputs.

The discussion of contextual setting was imperative for understanding how technology mediates with the everyday practices of a school. It depicts the 'site' where children lose their privacy rights. However, now it is important to understand the actors and their motivations/incentives for breaching children's right to privacy. While the first section of the chapter focuses on *where* privacy is lost, the next section shifts to *who* breach it, which is necessary to attribute liability and seek effective grievance redressal mechanism.

[323] Duggan, S. (2020). AI in Education: Change at the Speed of Learning. *UNESCO Institute for Information Technologies in Education*.
[324] Ayog, N. "Discussion Paper National Strategy for Artificial Intelligence." (2018).
[325] Ibid, p. 37

Education is a constitutionally mandated public welfare service under Article 21A of the Indian constitution. As a result, schemes like Sarva Siksha Abhiyan, Mid-Day Meals etc., have huge budgetary allocations by the centre towards different states.[326] Under these schemes, the government pays for teachers' salaries, cooked meals for children, scholarships to students and, in some cases, school uniforms and textbooks. For disbursal of such benefits, there needs to be streamlining of data about the beneficiaries' details which ensures the removal of unauthorised, duplicate, and fake applicants.[327] Research done by *Kumar and Rustagi* has shown that there are bogus claims of enrolment records shown by educational institutions to siphon additional rations of food and other materials from the government. This necessitates a secure system that aids the government in disbursal of public delivery services to schools.[328]

Aadhaar has been presented as the panacea for the leakages and wasteful expenditure that is happening due to inaccuracies in the school enrolment data. Proponents of Aadhaar state that, Aadhaar will plug problems regarding duplication and the multiplicity of educational records, but its opponents claim its capability of real-time data collection, storage, and sharing capabilities can breach an individual's right to privacy. Aadhaar is also used to plug almost all loopholes in the Indian education system - be it the dropout rate of students, teacher absenteeism, students' assessment results, examinations etc. Using Aadhaar for unintended purposes is also encouraged by state governments, for instance, state of Tamil Nadu (TN), which, through a circular, mandates all schools to collect Aadhaar details of the students.[329] The circular further mandates merging students' demographic and biometric details with the Educational Management Information Systems (MIS) - the state's centralised repository. As stated above, MIS is being maintained in several states, be it Tamil Nadu or in Gujarat, under the Gunotsav Scheme. These are centralised repositories of a particular school which are synchronised with the Unified District Information on School Education (UDISE) database, developed by the Ministry of

[326] Jaiswal, D, Sharma, E., Nath N., & Shekhar S., *An Analysis of Inefficient Allocation and Expenditure in the Education Budget,* Working paper, 334, Center for Civil Society.
[327] National Institute of Public Finance and Policy, "*A cost-benefit analysis of Aadhaar*", November 9, 2012, available at https://macrofinance.nipfp.org.in/FILES/uid_cba_paper.pdf, Accessed on 27th March 2021.
[328] Kumar, A. K., and Preet Rustagi. "*Elementary education in India: Progress, Setbacks, and challenges.*" (2010).
[329]Kaveri M, The News Minute, Aug 10, 2019, Available at, https://www.thenewsminute.com/article/tn-govt-makes-aadhaar-enrolment-compulsory-school-students-sparks-row-107004

Education.[330] Thus, integrating students' sensitive personal data, which is not limited to educational records, leads to further surveillance of children.

The act of integration or data aggregation begins with a socio-technical programme at the helm of all state government and central government policies, i.e., '*Aadhaar*'. Aadhaar means 'foundation' or 'bedrock' in several Indian languages. Aadhaar - a digital identity system came into existence in 2009 to enable targeted and efficient delivery of public welfare services. In 2010, the first Aadhaar was issued to a lady in the Tembhli, Maharashtra village after collecting her biometrics - photograph, fingerprints and iris scans.[331] Along with the biometrics, demographic information (name, age, gender, address) is stored in a centralised repository, managed by the Unique Identification Authority of India (UIDAI) - a body which owns, manages and operates the said repository, also known as, Central Identities Repository (CIDR). In essence, Aadhaar is not a document or an identification card, but a unique number allotted during enrollment and authenticated and verified at the time of provisioning of public welfare services.

It is essential to discuss *Aadhaar* separately because of its purported uniqueness and invisibility. Aadhaar is unique in its '*usage of algorithmic techniques of pattern matching*', which can identify, sorting and categorising individuals. At the micro level, the Aadhaar system collects and stores the personal data of individuals. When they approach to avail any public distribution service, like healthcare, education, banking etc., the system must identify the individual by comparing its information with the submitted data and authenticate the transaction. In this manner, each individual transaction with the state gets logged, the individual receives the service, and government plugs leakage in the supply chain and corruption in the system. In the school context, Aadhaar envisages a new policy dimension in improving child's education journey and school system transformation.

Aadhaar has a flip side to its operationalisation too. Aadhaar, asserted as a Digital Identification mechanism is more than that due to its unique technical abilities, and therefore should be seen as a socio-technical system. The intention of Aadhaar is to monitor the entire supply chain of any public distribution service and aid disbursal by verifying and authenticating an individual's identity. The collection of biometrics, its verification through data centres, storage at centralised

[330] DT Next, TN to launch all in one portal to track schools, 26th May, 2019, Available at https://www.dtnext.in/News/TopNews/2019/05/26045928/1139624/TN-to-launch-allinone-portal-to-track-schools.vpf.
[331] Sinha, K. (2023). A Matter of Identity. In *The Future of India's Rural Markets: A Transformational Opportunity* (pp. 23-26). Emerald Publishing Limited.

repositories and authentication in schools, hospitals, and ration shops (delivery sites), involve multiple layers of intermediaries through which the sensitive personal data passes. The Aadhaar system meant to minimise middlemen's role has, in fact, institutionalised the role of intermediaries. Such intermediaries are often invisible behind the technological layers, resulting in ineffective assistance in cases of non-delivery of public services. Aadhaar in educational space is similar to Foucault's '*Panopticon*', as it is unknown to the data subject how their data would be used, who will use it, and how it will be shared, resulting in minimal control over one's own information.[332] Similarly, Aadhaar is also an example of '*surveillant assemblage*' as it is built like a rhizome with its tentacles in every sector, collects a variety of personal information, operating under various actors, and governing the flow of data.[333] Thus, Part B is an attempt to connect Aadhaar with the surveillance theories presented in the first chapter and lay out Nissenbaum's second and third parameter i.e., the '*actors*' and '*information types*'.

2.1 Examining Aadhaar in the Educational Space

Under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, hereinafter Aadhaar Act, 2016, the Central Government of India mandates the usage of Aadhaar to avail of the benefits under any government scheme. In the school context, on 5th September 2018, UIDAI, through a circular, ensured that "*no children are deprived/denied of their due benefits or rights for want of Aadhaar - in terms of admissions, scholarships, attending various Board examinations, participating in various competitive examinations*".[334] However, the said authority, in the same circular, has also obliged schools to provide Aadhaar enrolment and biometric update facilities for those children whose biometrics are not updated in the Aadhaar Database.[335] The government presents the absence of Aadhar enrolment facilities in schools as a "*hardship to children*". It uses it as an opportunity to earmark the state budgets to fund enrolment

[332] Krishna, Shyam. "Identity, transparency and other visibilities: A liquid surveillance perspective of biometric identity." *Available at SSRN 4404834* (2019). The author leads to a similar conclusion of calling Aadhaar a panopticon, though not examined through educational lens.
[333] Again, Aadhaar has been touted to resemble the characteristics of assemblage but never examined through educational lens. See, Henne, Kathryn. "Surveillance in the name of governance: Aadhaar as a fix for leaking systems in India." *Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century* (2019): 223-245.
[334] F.No. 4(4)/57/146/2012/E&U, Government of India, Ministry of Electronics and Information Technology, Unique Identification Authority of India, available at https://uidai.gov.in/images/resource/Circular-School-06092018.pdf.
[335] This responsibility is levied by UIDAI on schools under Regulation 12A of Aadhaar (Enrolment and Update) Regulations to arrange for Enrolments and Biometric updation.

machines for capturing biometrics.[336] Since education is a state subject, state governments like Assam,[337] Punjab,[338] Tamil Nadu[339] have made it compulsory for students to enroll. The schools accept alternative Digital Identifications like passports, Birth Certificates etc., but the mandatory requirement by the central government makes other identifications meaningless. Furthermore, enrolling children on the Aadhaar programme is cumbersome as there are numerous instances of children not being recognised by biometric machines due to changes in their physical biometrics. It requires a child to be enrolled in Aadhaar at least three times[340] by the time one turns adult - before they turn five, between the age of six and seventeen and once they turn adult. Without an Aadhaar, it is practically impossible for a child to avail themselves of the benefits of any educational space as Aadhaar is being used as an identifier in respect of the following education-related schemes-:[341]

2.1.1 Centrally Sponsored Scheme for providing quality education in Madrasa (SPQEM)[342]

This scheme aims to bring quantitative and qualitative improvement in Madrasas by introducing formal subjects like Hindi, English, Science etc., and simultaneously providing access to science labs, libraries, computer resources and online learning materials. The government also intends to provide a higher honorarium to teachers so that better quality teachers would be interested in applying for the positions inside Madrasas. However, to access student learning resources, honorarium for teachers and scholarship funds for the needy, each needs to enroll in the Aadhaar programme. Herein, the Aadhaar system integrates with the student and teachers' financial

[336] UIDAI offers 200 crore assistance to states to fund enrolment machines in sub-districts that can be used for Aadhaar enrolment. This move came just days after the UIDAI's circular asking schools not to reject students for lacking an Aadhaar number. Available at https://uidai.gov.in/images/news/Rs200crore-earmarked-to-fund-Aadhaar-enrolment-machines-for-schools-MPost.pdf.

[337] Under *Axom Sarba Siksha Abhijan Mission*, the process of distribution of free Aadhar cards has started under which, if any student has an Aadhaar number can avail of services of a free bank account. Available at https://www.eastmojo.com/news/2020/11/09/free-aadhaar-cards-for-assam-school-students/.

[338] From April 1, 2021, the Punjab Schools are obliged to undergo Aadhaar biometric updation from primary school students to senior secondary school students. Available at https://www.tribuneindia.com/news/schools/punjab-school-education-department-directs-for-biometric-updation-in-aadhaar-cards-of-students-226135.

[339] On August 2, 2019, the school education department of Tamil Nadu through a circular pushed for Aadhaar enrolment for school students under the "*Samgra Shiksha Abhiyan*" which covers 58,474 schools and over 1.23 crore students. Available at https://www.eastmojo.com/news/2020/11/09/free-aadhaar-cards-for-assam-school-students/.

[340] Yadav A., *Parents struggle to sign up infants*, Identity Project, Aug 29, 2016, Scroll, Available at, https://scroll.in/article/814891/parents-struggle-to-sign-up-infants-toddlers-for-aadhaar-as-centre-eyes-100-enrolment-by-march

[341] Press Information Bureau, *Aadhaar for social welfare*, Ministry of Education, 31st July, 2017, Available at, https://pib.gov.in/PressReleseDetail.aspx?PRID=1497803.

[342] http://egazette.nic.in/WriteReadData/2017/175554.pdf.

records in case of scholarship and granting honorarium, respectively. If a student does not have a personal account, the personal details of the guardian and their Aadhaar details will have to be shared for scholarship disbursal.

2.1.2 Mid-Day Meal Scheme (MDMS)[343]

The Mid-Day Meal scheme provides healthy food to improve the nutritional status of children studying in classes I to VIII in government or government-aided schools or Special training centres or Madrasas or Maqtabs under the Sarva Shiksha Abhiyan. This aligns with the Conventions of the Rights of Children (CRC),[344] where India has committed to providing adequate and nutritious food to primary and upper-primary students. The food is provided during working days and, in some states, even during the summer vacation period. The intention behind starting this scheme was to encourage more enrollment of students, especially from the poorer sections of society. The Department of School Education & Literacy under the Ministry of Education, through a notification dated 8th June 2017, released a format to capture the school-wise Aadhaar Enrolment data through the MDM-MIS portal (Mid-Day Meal - Management Information System).[345] The provisioning of meals is inextricably linked to the Right to Education under Article 21-A of the Indian constitution, which is a fundamental right to provide state-funded education. The right's provisioning is now subject to enrollment in the Aadhaar system. It raises the question of whether a fundamental right guaranteed by the constitution should be subjected to a mandatory requirement established by the executive notification. Though the question is not directly the subject matter of this thesis, the ICCPR casts an obligation on the states to respect the government mandate to protect the rights of individuals.[346]

---

[343] Available at, http://egazette.nic.in/WriteReadData/2017/174505.pdf.

[344] Article 24, Paragraph (c).

[345] F. No. 9-3/2017-Desk (MDM) Government of India, Ministry of Human Resource Development, Department of School Education & Literacy, Available at, https://pmposhan.education.gov.in/Files/OrderCirculars/2017/Lt_on_Aadhaar_Enl_dataEntry.pdf.

[346] Also, the Indian Supreme Court in *Behram Khurshed Pesikaka v. The State of Bombay*, (1955) 1 SCR 613, stated that *fundamental rights are sacrosanct and are not to be capable of being waived. It is the duty of the state, through the constitutional preamble to protect individuals from any interference and operationalise the individual benefit to secure justice*. Thus, mandatory requirement of Aadhaar to avail a constitutional fundamental right, should be viewed as a unconstitutional requirement. For more analysis on Aadhaar's linking with Mid-Day Meal scheme refer to, https://blogs.lse.ac.uk/southasia/2017/06/26/aadhaar-and-the-mid-day-meal-scheme-a-denial-of-basic-rights/ and https://www.hindustantimes.com/opinion/aadhaar-linked-to-mid-day-meal-why-put-the-burden-on-children/story-Z7E1vk4g7kOyk3FKRKwkoN.html.

2.1.3. Sarva Shiksha Abhiyan (SSA)[347]

This central-level scheme universalises elementary education in India and acts as a vehicle for implementing the RTE Act. For such purposes, there are multiple targeted interventions in schools, like the construction of additional classrooms, toilets, facilities for drinking water, resource support for academics, and uniform and teacher training. Since the RTE act applies to children within the age group of 6 to 14, thereby, such students must be enrolled in the Aadhaar Programme to avail of benefits and entitlements. Further, teachers and staff (called functionaries in the notification) must also be enrolled to avail of salary, honorarium, and other benefits. Under this scheme, the date of birth is captured through the Aadhaar system, based on which the student is admitted to a school. The demographic details of the parent/guardian are captured and stored to verify the addresses and pin codes so that the student is enrolled in the nearby locality. Once the school is chosen, the online form asks for sensitive details irrelevant to the child's educational journey, like parents' caste and income certificates. The said details are further cross-checked with the revenue department's database. Such online forms are filled in the offices of Block education officers where students' fingerprints are recorded for 'official use' and verified against the Aadhaar database.[348] Thus, a student's data along with their parents is shared across departments, verified across the Aadhaar system, and thereby is an amalgamation of sensitive personal details, captured without any legal framework in place.

2.1.4 Inclusive Education for Disabled at Secondary Stage (IEDSS)

This scheme is established under the Rashtriya Madhyamik Shiksha Abhiyan to cater to the educational needs of Children with special needs in the age group of 14 to 18 and studying in classes IX to XII. Children with special needs are defined as having one or more disabilities as defined under the Persons with Disabilities Act, 1995, namely, i) Blindness, ii) Low Vision, iii) Leprosy cured, iv) Hearing Impairment, v) Locomotor disabilities, vi) Mental retardation, vii) Mental Illness, viii) Autism, and ix) Cerebral Palsy. It can be inferred that under this scheme, various kinds of sensitive personal information is stored like Health details, demographic details, name, gender etc. Mandating Aadhaar to avail benefits under this scheme means that such sensitive information is stored in a centralised repository and interoperable with other government and

[347] Available at, http://egazette.nic.in/WriteReadData/2017/174484.pdf.
[348] RTE Linked to Aadhaar to avoid duplication, The Times of India, Feb 28, 2018, Available at, https://timesofindia.indiatimes.com/city/bengaluru/rte-linked-to-aadhaar-to-eliminate-duplication/articleshow/57381223.cms.

private players. Such storage and sharing norms hold the potential to lead to biases in a country like India which is riddled with social prejudices, especially regarding disabilities.

2.1.5. Saakshar Bharat[349]

The Ministry of Education implements a centrally sponsored adult education and skill development scheme called Saakshar Bharat. Under this scheme, basic literacy and numeracy are provided to adult non-literates in the age group of 15 years and above and provide basic education opportunities to neo-literates and school dropouts through Continuing Education Programme. The government provides literacy primers and other training materials through different State's Literacy Missions. Voluntary teachers build these primers and materials for which the Central government does not pay any honorarium. Still, respective state governments can hire the services of additional teachers, trainers, and Village Level Coordinators (called 'Preraks') on a monthly honorarium. Every child and other beneficiaries must enroll for the Aadhaar Programme to avail of such benefits.

Further, under the aegis of this scheme, the Central Government also supports NGOs/Institutions/State Resource Centres for skill development to adult neo-literates and other targeted beneficiaries. These State Resource centres function under the Registered Voluntary Agencies or Universities and receive grants under the scheme. This scheme allows them to map those students who are not enrolled in the Aadhaar database due to being illiterate or dropping out of school/college. Thus, the Aadhaar database is rhizomatic in nature, like a surveillance assemblage, which leaves no student in its temporality.

2.1.6 National Means-cum-Merit Scholarship Scheme (NMMSS)[350]

Specific schemes allow beneficiaries to avail themselves of scholarships and support their education through those entitlements. However, to receive a scholarship, the student has to complete the Aadhaar Card registration to seed it with the bank account, which enables Direct Benefit Transfer (DBT). Apart from NMMSS, other sector-specific scholarship schemes like INSPIRE (Innovation in Science Pursuit for Inspired Research) and DISHA scheme allow middle school students to opt for science research. Some states use a consent form to seek acceptance of Parents/Guardians permitting the use of an Aadhaar Number in case of a State Scholarship

[349] Available at, http://egazette.nic.in/WriteReadData/2017/174524.pdf.
[350] Available at, http://egazette.nic.in/WriteReadData/2017/174187.pdf.

Application.[351] Thus, there are two different storage repositories, which are interoperable: one at the central level, where the UIDAI manages all the Aadhaar details, and the other at the state level, where the state government manages all details related to Caste, Income Certificate, Contact Address, Name, Pincode etc.

The schemes enable the central government to accumulate complete information about each student, irrespective of which state one resides, and store it in an aggregated format, resulting in an '*Education Stack*'. Reflecting on the above-mentioned schemes, it can be deduced that students and teachers are at the centre of the Aadhaar system that renders the school a panopticon. Such a panopticon is developed due to the state-sanctioned data-driven exercises operated through invisible intermediaries. The usage of the technology is disguised in the name of improving learning competencies, providing education to all, or providing financial aid to the marginalised section of the population.

2.2. MOTIVATIONS BEHIND CONSTRUCTING '*EDUCATION STACK*' IN SCHOOLS

The chapter now lays down the motivations and incentives for the state to design, develop and deploy technologies. Understanding such reasons is essential to navigating the necessity, reasonableness and proportionality of any technology's design, development and deployment in a given context.

2.2.1 Students and Teachers at the Centre

The Indian government's National e-governance plan (NeGP) has a clear vision to make education available to all children smoothly and transparently.[352] In 2015, India also adopted the 2030 Agenda for Sustainable Development, in which India seeks to achieve Goal 4 to "ensure inclusive and equitable quality education and promote lifelong learning opportunities for all". To achieve this goal, the National Education Policy (NEP) 2020 states that "*teachers must be at the centre of the fundamental reforms in the education system*". It further states: NEP "*must help re-establish teachers, at all levels, as the most respected and essential members of our society because they shape our next generation of citizens*". The idea is to evaluate teachers'

[351] Consent Form by Parent/Guardian permitting use of Aadhaar/EID Numbers submitted in the State Scholarship Application, Available at, https://ssp.karnataka.gov.in/images/consente.pdf.
[352] Saaransh, MeitY, Bird's eye view of all Mission Mode projects, Available at, https://www.meity.gov.in/writereaddata/files/Compendium_FINAL_Version_220211(1).pdf, p. 77.

performance through real-time monitoring and based on the available data, recruit the brightest faculty available for the teaching profession. This is thought to maintain transparency, fairness, and accountability in the education system. The government believes that real-time monitoring is possible only through integrating technology with each aspect of education - like curriculum, enrollment of children, school governance, assessment, peer interactions etc. - each layer contributing to the Education Stack.

2.2.2 Standardisation of Learning Competencies

One of the primary goals of NEP 2020 is to bridge the "*gap between the current state of learning outcomes and what is required*". For such purposes, the government under NEP intends to set up a normative standard upon which an Accreditation would be given to a particular school or Higher Educational Institution (HEI). For such purposes, the government proposes to set up PARAKH (Performance Assessment, Review, and Analysis of Knowledge for Holistic Development) - a National Assessment Centre to set up standards and guidelines for "*student assessment and evaluation"*.[353] The proposed PARAKH will gather and sort data from E-Learning management systems (centralised repositories in each school) already established in rural and urban schools by Aadhaar. Advanced learning management systems (LMS) are used because they can store personal and non-personal information in a centralised place, and it's used by educational authorities to automate administration.[354] It further personalises the content like course content, quiz, tests, assignments, and surveys and improves tutor-learner interaction based on the personal information collected and aggregated.

Advanced LMS can help schools and, thereby, the government to gain greater feedback on both the student and teacher, comparative assessment of a particular student, insights on course instructor engagement and delivery, and student's learning outcomes and satisfaction. Such collection and processing through a single command and control centre aid the government in capturing the above insights and storing massive troves of data needed on each student. For instance, the Gujarat government saw an opportunity to build a functional architecture of a repository entailing all details of students and teachers in the state. Much before NEP 2020, the Gujarat government in 2009 brought Gunotsav (Guna [Goodness] + Utsav [Celebration]) project

[353]Indian Express, *NEP roll-out,* October 15, 2020, Available at, https://indianexpress.com/article/education/education-ministry-world-bank-launch-rs-5718-crore-project-to-improve-school-education-in-6-states-6724978/.
[354] Ellis, Ryann K. "Learning Management Systems." *Alexandria, VI: American Society for Training & Development (ASTD)* (2009).

under the "*Samagra Shiksha*" scheme to set standards for learning and assessment in the state of Gujarat.[355] Under this scheme, the state-level education officers receive first-hand information through the education department's Command and Control Centre (CCC). The CCC provides real-time data from databases (like Advanced LMS, which have been integrated with U-DISE and Aadhaar) and covers "*62 lakh students, 2.5 lakh teachers, 3250 cluster resource coordinators (CRCs) and 263 block resource coordinators (BRCs) and 40,300 schools across 33 districts*".[356] Under this scheme, the Gujarat Education Department is a Registrar, and school principals, BRCs, CRCs, and district officials act as Introducers. Further, the Gujarat government has roped in Microsoft[357] to aid and assist the CCC in maintaining an online dashboard which will process the data collected to yield its evaluation, usability, and effectiveness in terms of the performance of teachers and students.

2.2.3 Institutional Processes and Protocols

Generally, the functional architecture of deploying and operationalising biometric technologies involves four entities (herein, we discuss the '*invisible intermediaries*' in an Aadhaar system, but it can apply to any design and deployment of a technology):

1) **Registrar** - It is an agency authorised by the State or Central Government or any public sector undertaking hired for enrolling individuals for biometrics. In the case of the education sector, it is the State Education Department or the Ministry of Education. There would be a Registrar and a few Sub-Registrars in the departments like the Deputy Commissioner, district collectors, etc.

2) **Enrolment Agencies** - The respective sectoral registrars hire enrolment agencies to collect biometrics and demographics. The Indian government intends to decrease the involvement of private enrollment agencies like 4GID Solutions Datasoft, Spanco, UTI Technology etc.[358] Rather, the government has asked the public sectors banks like State Bank of India, Punjab National

[355] This scheme was brought by the then Chief Minister of Gujarat and currently the Prime Minister of India, Shri Narendra Modi. The Gujarat government has brought this scheme to replicate U.K. 's initiatives of inspecting and assessing the educational standards of schools and colleges set up by the UK's Office for Standards in Education (Ofsted).
[356] Sharma R., *Teacher, student, schools to be tracked*, Indian express, Sept 19, 2020, Available at, https://indianexpress.com/article/education/gujarat-teachers-students-schools-to-be-tracked-to-analyse-online-classes-6601875/.
[357] Ibid.
[358] Economic Times Tech, *200 agencies to enroll citizens for UID*, Jul 16, 2010, Available at, https://economictimes.indiatimes.com/tech/software/200-agencies-to-enroll-citizens-for-uid/articleshow/6173502.cms?from=mdr.

Bank and certain private sector banks to offer Aadhaar enrolment and updation facilities.[359] However, with no law requiring the deletion of data on being removed as an agency, it runs the risk of data retention by earlier private partners.

The Enrollment agencies hire Operators and Supervisors to execute enrolment at the enrolment centres and manage these, respectively. Operators are key to the entire process as they directly engage with citizens in capturing biometrics and other details, taking consent from the individual and allowing the Digital ID. Enrolment agencies are important to verify and authenticate the submitted information in the data collection stage. Thus, in the event of non-authentication of a student while availing of any public service, the agency should be liable.

3) **Introducers** - Individuals (like the school's headmaster, teachers, and local NGO representatives) enlisted by the Registrar to spread awareness of a particular program by organising workshops. Further, on the day of the enrollment, they also act as verifiers of the information any resident supplies, like Name, Address. Further, the Introducer must provide her/his biometrics to log in to the computer to authenticate the biometrics captured by the Operator.

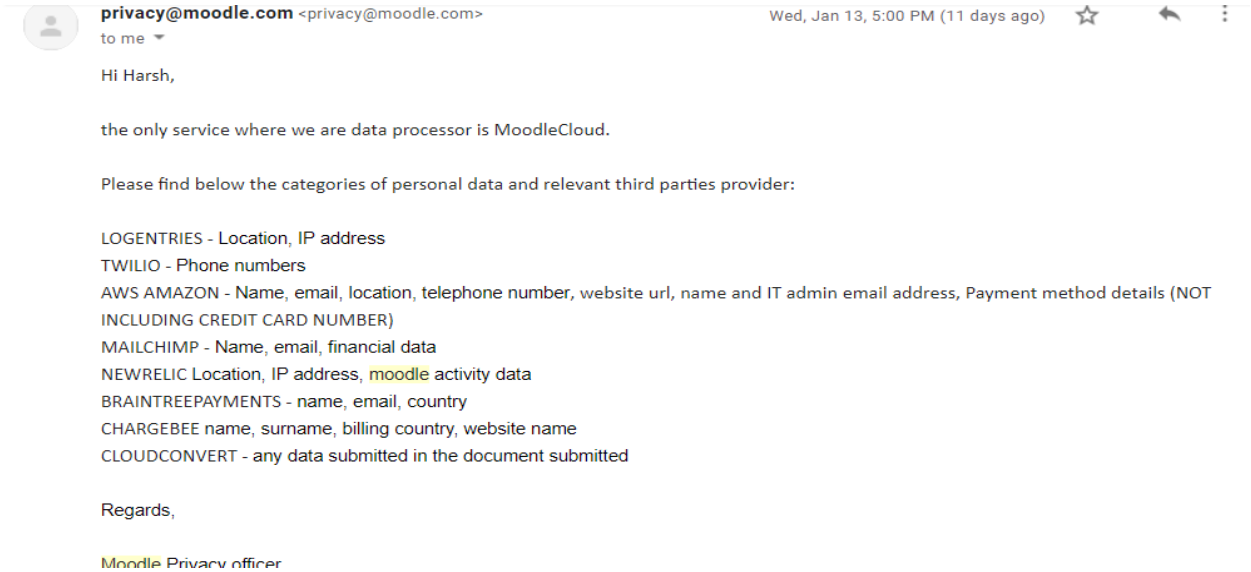
Apart from the stakeholders involved in the operationalisation of biometric machines and enrolment centres and campaigns, public and private vendors are involved in manufacturing, supplying and installing biometric machines and software. For instance, a Right to Information I filed to the Directorate of Education of Delhi revealed that the Delhi government chose Technosys Security Systems Pvt. limited to supply, install, test and commission CCTV cameras embedded with facial recognition systems and other allied infrastructure. Similarly, UIDAI awarded contractual tenders to the trio consortium - Accenture, Mahindra Satyam-Morpho and L1 Identity Solutions - to manufacture and install biometric identification systems for the Aadhaar programme.[360] During the initial days of Aadhaar, it was also reported that Ernst & Young had been hired for their consultancy services to provide an implementation strategy of CIDR - as

[359] Sharma A., Govt. *plans to limit role of private agencies in Aadhaar enrolment*, Economic Times Politics, Sep 08, 2017, Available at, https://economictimes.indiatimes.com/news/politics-and-nation/government-plans-to-limit-role-of-private-agencies-in-aadhaar-enrolment/articleshow/60415970.cms?from=mdr.
[360] Moneylife Digital Team, *UIDAI not so clean partners and their tainted executives*, 15th November, 2010, Available at, https://www.moneylife.in/article/uidais-not-so-clean-partners-and-their-tainted-executives/.

earlier explained, a centralised repository where all biometrics are preserved.[361] Based on this understanding, the entire Aadhaar system is a surveillant assemblage - comprising a network of public and private actors - through which all the personal data is navigated, leading to a Chresthomatic Panopticon.[362]

2.2.4 Data-Driven Exercise

Programs/schemes/projects like Gunotsav showcase the harms of integrating Advanced LMS with other technological systems (like Aadhaar) and private vendors (like Microsoft) without understanding the latter's terms of use and privacy policies. For instance, during my research, I contacted '*Moodle's*' privacy officer (widely used LMS in India) and asked about the categories of personal data for which they rely on third-party sites:



privacy@moodle.com <privacy@moodle.com> Wed, Jan 13, 5:00 PM (11 days ago)
to me

Hi Harsh,

the only service where we are data processor is MoodleCloud.

Please find below the categories of personal data and relevant third parties provider:

LOGENTRIES - Location, IP address
TWILIO - Phone numbers
AWS AMAZON - Name, email, location, telephone number, website url, name and IT admin email address, Payment method details (NOT INCLUDING CREDIT CARD NUMBER)
MAILCHIMP - Name, email, financial data
NEWRELIC Location, IP address, moodle activity data
BRAINTREEPAYMENTS - name, email, country
CHARGEBEE name, surname, billing country, website name
CLOUDCONVERT - any data submitted in the document submitted

Regards,

Moodle Privacy officer

Based on the above e-mail communication and a few other studies on Moodle LMS, the following table showcases the information types that can be stored on an LMS and shared with third parties:

S. No.	Type	Information	Sensitivity in Terms of Privacy and Confidentiality

[361] The Hindu, *E&Y selected as consultant for UIDAI*, Feb 26, 2010, Available at, https://www.thehindu.com/news/national/Ernst-and-Young-selected-as-consultant-for-UIDAI/article16817121.ece.
[362] Supra, refer to Chresthomatic Panopticon, Second Chapter, Part B.

1.	Personally Identifiable Information (PII)	Date of Birth, Nationality and native language, postal address, phone number, e-mail address, learner school ID (contains a photo and other demographic details, or maybe a Unique identity number too), special conditions assigned with the learner (any disability), payment method details	Very High
2.	Course Data	Registered modules/courses, completed course results, assignment details submission, course settings, and list of participants.	Low
3.	Learning Data	First phase - Emotional Data, Planning Data Second Phase (*Performance Data*) - audio or video recordings, levels of participation, and time spent on tasks. Third Phase (*Reflection*) - Feedback by teachers /Peers/Parents to students (irrespective of a classroom setting, space or time)	High
4.	Personal Notes	Annotations, Notes on Google Keep, personal messages/remarks on LMS forums, self-assessments, collaborative assignments, and reflections.	High

Reflecting on these developments and placing them in the Indian context proves what *Jacques Ellul* argues in the context of technological developments in Post-War France - i.e. '*the state had become an enormous technical organism*'.[363] He further observes '*political doctrine no longer represents the end; the autonomous operation of techniques represents the end*.'[364] The advent of computerisation, biometric technologies, and Artificial Intelligence has not only led to the restructuring of state-government relations, i.e. state contract theory, but also made citizens completely visible - to what *Anderson* states as "*total surveyability*"[365] - a condition in which technologies are used to track, map, tag, categorise and profile individuals by building vast repositories of both personal and non-personal data. In India's case, the state, while grappling with the idea of a technological society, captured the idea of *Aadhaar* through which the entire scope of life falls under technological imperatives and, thereby, the state's lens. The operation of various actors, cutting across the entire education sector, collection of invasive personal data, and the presence of power asymmetry between the data subject and controller makes Aadhaar a panopticon, a tool of surveillant assemblage and surveillant capitalistic, endangering the privacy rights of students. This is further detailed out in Part C.

PART C - IMPLICATIONS OF 'EDUCATION STACK' on RIGHT TO PRIVACY

3.1. Implications of Data Production Behind School Doors

A surveillance society amalgamates techno-bureaucratic-entrepreneurial norms, primarily for identifying citizens in a given space. Such identification happens through continuous monitoring, data collection, processing, and sharing. It also enables hierarchising individuals based on their caste, colour, place of birth, gender, occupation, affluence, etc. Platforms like Aadhaar, enmeshed with economic and political motives, constitute and (re)shape technological infrastructures. These platforms should be understood as a site of interactions between the platform producers and consumers. For instance, if schools are the consumers, the government or private players will be the producers. Platforms are built over an existing 'infrastructure' like the Internet, data centres, open data standards or smart devices. However, with the arrival of Aadhaar, it has reconceptualised the meaning of platform as it can perform the dual role of both platforms and

[363] Ellul, Jacques, John Wilkinson, and Robert King Merton. *The technological society*. Vol. 303. New York: Vintage books, 1964, p. 252.
[364] Ibid, p. 282
[365] Anderson, B. (2006)., Census, Map, Museum, *imagined communities: Reflections on the origin and spread of nationalism*. Verso books. p. 189.

infrastructure. Aadhaar as a platform brings together and authenticates citizens, market players and government agencies. As an infrastructure, it enables the government to carry out governance and market players to organise economic activities and enables datafication of individuals leading to a surveillant state. The seeding of Aadhaar in several educational and governmental policies, which already link and store burgeoning non-educational data treat data emanating from the schools as an economic asset. It is complemented by privatising public welfare services and the absence of any framework to regulate data collection, processing, sharing, and storing.

As we saw in the first chapter, Foucault defines power in the disciplinary sense but also formulates a positive conception of power in his book '*Archaeology of Knowledge*' which moves away from repression, subjugation, exclusion and marginalisation to observation, production of knowledge and multiplication of its effects by combining observation and knowledge.[366] Aadhaar is also a site of knowledge production and distribution - production of states, nation, and people; distribution of identities - that aids the government in nation-building and disbursal of services but also become sites for classification, exclusion, displacement and profiling.[367] Due to the troves of information stored on Aadhaar sites, the government has exclusive power over its citizens. Further, due to the state-private nexus, private companies and private school administrations can also exercise and tighten control over students.

3.2. Surveillant Assemblage behind biometric technology

The primary purpose of biometric technologies has been an individual's unique identification, as stipulated by Article 4(14) of the GDPR. The identification history of biometrics can be traced back to pre-colonial India, where fingerprints have been used for seals and signatures.[368] Other forms of identification, including tokens, legal names, and ration cards, were acceptable too. However, each form of identification is susceptible to a front-end problem of bogus cards, duplicity in biometrics and a back-end problem of corrupt practices by the stakeholders involved. *H.K.*

[366] Michel Foucault uses the term power in the disciplinary lens when power is used for subjugating the bodies under routine practices, procedures which turn the bodies 'docile'. Foucault's earlier works like Madness and Civilization, The Birth of a Clinic and The Order of Things can also be read for this understanding. *Supra*, Chapter 1.
[367] Arjun Appadurai, '*Number in the Colonial Imagination*', in Carol Breckenridge and Peter Van Der Veer (eds) Orientalism and the Postcolonial Predicament: Perspectives on South Asia, Philadelphia: University of Pennsylvania Press, 1993, pp. 314–339.
[368] Waits, M. R. (2016). The indexical trace: a visual interpretation of the history of fingerprinting in colonial India. *Visual Culture in Britain*, *17*(1), 18-46.

Bhabha merges these problems and terms as an "*Entstellung - a process of displacement, distortion, dislocation, repetition*".[369] British India wanted to regulate the '*chaotic diversity*' of tax collection and policing.[370] *William Herschel*, a civil servant, emphasised the colonial government to use palm vein and fingerprinting technology to authenticate the colonial subjects for running the economy as it would prevent duplicitous claims.[371] However, it was post-development of the classificatory fingerprinting system by Edward Richard Henry that fingerprinting was used as a ubiquitous mechanism by the British colonial government.

According to Mordini and Massari, any measurable parameter in our body is capable of being converted into a *standardised unit of measurement* as biometrics have four characteristics: a) *Collectability* - The parameter (finger, palm, face, iris, emotion etc.) can be captured, b) *Universality* - The parameter is universal in all individuals irrespective of class, caste, gender, place of birth etc., c) *Unicity* - The chosen parameter is unique to each individual, and, d) *Permanence* - The parameter remains permanent over time.[372] Biometric technology is seen as a potential governance tool as its measurable characteristics elicit participation, engagement, discussion, transparency and accountability of all societal actors, whether the state or the citizens. Biometric technology brings with it actors like private entities to capture and control citizens' information legally and formally, giving rise to digital infrastructures enabling state surveillance. Contrary to participation and engagement, biometric technologies create a norm-governed system in which the citizens are at the mercy of the state. The types of data that shall be triangulated, merged, and processed are governed by the norms and citizens are disciplined by those norms.

In the aftermath of the September 11 attacks, it was clear that human security posed severe challenges to the myriad conceptions of national security.[373] Technology came to the rescue as it was touted as a security and risk assessment tool, making the processes transparent, determinate and faster. The panic campaigns orchestrated by the state and its agents, multiplied

[369] Bhabha, Homi K. "Signs taken for wonders: Questions of ambivalence and authority under a tree outside Delhi, May 1817." *Critical Inquiry* 12, no. 1 (1985): 144-165.
[370] Sengoopta, Chandak. "Treacherous minds, submissive bodies: corporeal technologies and human experimentation in colonial India." (2018).
[371] Singha, Radhika. "Settle, mobilise, verify identification practices in colonial India." *Studies in History* 16, no. 2 (2000): 151-198.
[372] Mordini, Emilio, and Sonia Massari. "Body, biometrics and identity." *Bioethics* 22, no. 9 (2008): 488-498.
[373] Lyon, D. (2003). *Surveillance after September 11* (Vol. 11). Polity.

by the media, gave rise to biometric governmentality around the globe.[374] In the Indian context, Nandan Nilekani propagated the idea of a Biometric National ID - '*Aadhaar*' - which he says could prove to be transformational by improving the quality of public services and increasing inclusivity and equality by enabling the reach of services to citizens.[375] Nilekani provided recourse to an anxious Indian government which, in 2011, in its National e-Governance Plan[376] highlighted the issues of fake and duplicate cards in the Public Distribution System (PDS).[377] It further stated that unauthentic cards lead to diversions of rations to phantom identity holders and result in inefficiency. Nevertheless, the introduction of Aadhaar is not limited to PDS but is linked to tax, housing, employment, and other related schemes in the education sector. This has resulted in a '*biometric panopticism*' not only to authenticate, match and verify individuals in a society to avail certain services but create a memory of the individual identity and each of its transactions by storing information in a centralised repository (in the case of Aadhaar, it is the Centralised Identities Repository - CIDR).

Similar governance anxiety can be traced back to introduction of facial recognition systems (FRS) and Emotional AI technologies in education. As stated by the Hon'ble Minister of Home Affairs on 2nd February 2021 before the Indian parliament, FRS was deployed at the discretion of the state government for law and order, protection of the life and property of the citizens, including investigation and prosecution of crime.[378] Maybe, the deployment of FRS systems is understandable in the United States because of several school shooting incidents.[379] However, in India, where there is a strict gun control law in place, the safety and security of students are far less complicated, and there is no necessary, legitimate and proportional need for any biometric technology (explained in detail in the sixth chapter).[380] For instance, the Delhi government claims to install FRS embedded in the CCTV cameras for the safety and security of children and fast-tracking the attendance of students. Furthermore, COVID-19 has paved the way for state

[374] Hope, A. (2015). Governmentality and the 'selling' of school surveillance devices. *The Sociological Review*, *63*(4), 840-857.
[375] Nilekani, Nandan. *Imagining India & Ideas for the New Century*. Penguin Books India Pvt. Limited, 2008.
[376] Supra note 308, *Saaransh: A compendium of Mission Mode Projects Under NeGP, Government of India*. https://www.meity.gov.in/writereaddata/files/Compendium_FINAL_Version_220211(1).pdf.
[377] In India, through the public distribution system, subsidised food rations are provided to people below the poverty line.
[378] http://164.100.24.220/loksabhaquestions/annex/175/AU191.pdf.
[379] Andrejevic, M., & Selwyn, N. (2020). Facial recognition technology in schools: Critical questions and concerns. *Learning, Media and Technology*, *45*(2), 115-128.
[380] The three-prong test of legitimacy, necessity and proportionality is detailed out in Chapter 6.

governments to increase school surveillance when the entire education market has turned digital.[381] Under the Kerala Information Mission, the state government of Kerala have deployed a Radio Frequency Identification system.[382] It claims to '*reduce the distance between home and school*' by tracking the child's movement both within and outside the school. The real-time info generated by the RFID tag gets transmitted to the parent's mobile phone or e-mail.

For a particular program of deployment of any technology in a school, several stakeholders form part of a regulatory structure: *Enrolment agencies, Registrars, Public or Private vendors, IT Consultants, Training and Logistics organisations and facilitation authorities* (like principals, teachers at particular school) forming a network of agents, i.e. a 'surveillant assemblage'. Without a data protection regulation, the personal information of a child passes through a centralised architecture riddled with functional middlemen who continuously identify, categorise, sort and profile a child without its consent.

We can appreciate the notion of digital governance through Althusser's construction of an institutionalised 'state apparatuses'. Althusser divided a state apparatus into two: repressive state apparatus (RSA) and an '*Ideological state apparatus*' (ISA).[383] According to Althusser's Marxist conception, while the ruling class uses prohibitionary or punishment mechanisms in the case of RSA (courts, police, army etc.), through the ISA, the state incites, reinforces, moulds, optimises, organises and promotes its own beliefs/ideology (church, legal system, family and schools). Thus, Althusser considers institutions to exert power over the proletariat through repression or ideology. Michel Foucault's conception of '*Governmentality*'": which combines government and rationality where the state uses disciplinary means to control, shape or guide the population goes against Althusser's state apparatus theory.[384] Foucault disagrees with only state possessing a form of power, rather extending the limits of the state apparatus by conceptualising 'micro-physics of power'. Foucault describes micro-physics by tying scientific management and technological development, i.e., power is not possessed by the state but rather exerted strategically and tactically to dominate the subject. Foucault, through the different conceptions of power like

[381] Sunil MK, Govt schools get smart with RFID Badge in Kerala, Aug 13, 2015, Available at https://timesofindia.indiatimes.com/city/kochi/Govt-schools-get-smart-with-RFID-badge-in-Kerala/articleshow/48465037.cms.
[382] Ibid.
[383] Althusser, Louis. "Ideology and Ideological State Apparatuses [1970]." *Trans. Ben Brewster. The Norton Anthology of Theory and Criticism. Ed. Vincent B. Leitch. New York: Norton* (2001): 1483-1508.
[384] Özpolat, G. (2020). Bringing Althusser and Foucault Together: A Brief Overview of the Question of the State. *POSSEIBLE*, (18), 7-17.

biopower, pastoral power, governmentality, or disciplinary power, shows that power is relational and exercised in different shapes and forms, dependent on a context. Foucault's panopticon theory argues conceptualisation of power as dualistic (watcher exerting over the watched), but Nissenbaum theory of contextual integrity directs the power to be decentralised, i.e., power relations traverse the entire society and are shaped by everyday experiences, marginal institutions, family conditions and workplace environments.[385]

Different forms of technologies, when deployed in educational settings, should not be read in isolation as exerting repression over students, rather should be juxtaposed with the dense network of ancillary factors within which it operationalises. The second chapter explores the technologies exerting power in schools and the contextual setting in which they are deployed, thus considering the ancillary factors within which power gets 'cooked'. Understanding the power and its relationalities in a school opens the question of autonomy, secrecy, intimacy, and the information asymmetry that are different conceptualisations of the right to privacy.

Technologies per se do not understand societal dynamics and are at the mercy of the knowledge and creativity of their maker - the market forces. So, when the market enters the classroom and brings technology to discipline students, grade them, revise the curriculum, predict whether a child will drop out, or gauge students' attentiveness, the market biases enter a classroom too. This is the surveillance capitalism that first enters the school territory, accumulates children's data, unleashes predictions, coerces the school administration, guardians, and children to rely on those predictions and normalises the entire process for such technologies and forces to become a norm.

3.3. The Problem of Personally 'Identified' and 'Identifiable'

Flowing from the above discussion, Aadhaar is a site where every data comes together. It is a site of data aggregation where bits and pieces of data stored in decentralised government databases come together to frame a portrait of an individual. The power of aggregation in the digital age has multiple due to technological advancements, low computing power and inexpensive data storage abilities.[386] A piece of information in isolation might not be able to identify an individual personally, but when aggregated together can identify and reveal new insights about an individual. For instance, capturing a student's learning records and storing them in a school

[385] Oksala, J. (2016). Microphysics of power. *The Oxford Handbook of feminist theory*, 472-489. Also, for Foucault's panopticon theory, see discussion Supra, Second Chapter, Part B, section 2.2.
[386] Solove, supra note 143.

database might not be privacy intrusive, but mediating it through Aadhaar makes the personal attributes of a child visible.

Undoubtedly, combining data, processing, and analysing has its own benefits. Providing customised recommendations depending on students' abilities, a teacher focusing on a particular student in need of learning growth and predicting the drop-out rate of a student are laudable efforts for which AI technology can be used. But an AI is susceptible to yielding wrong predictions as it cannot feed into the contextual variations of a given society in which it operates. Data aggregation is a tool for surveillance by which the data aggregator can exercise control and make judgements about an individual. For instance, banks and insurance companies can use financial records to assess the creditworthiness of an individual. Similarly, education records can be used to assess whether a student should be given admission or a scholarship. However, data compilations, like financial and educational records, often need to be completed, as the data in such compilations is disconnected from the various social factors that design a contextual setting. Such wrong predictions generate physical, social, mental and dignitary harm coerced upon a child. A student gives bits of information at each stage of schooling without knowing how that data would be used to make predictions about them. But the aggregator consolidates power over the data subject, leading to a loss of control over their own information, subsequently giving rise to information asymmetry.

Data aggregation does not always lead to the identification of an individual but can be one source of identification. The identification process can be inherently damaging to the autonomy and, thereby, the privacy of an individual when it limits to means of identification. For example, in the case of Adhaar, it is the only mandatory means to avail public services, like admission to a school. Similarly, fingerprint scanners are necessitated in schools for attendance purposes, again snatching the liberty and autonomy feature of privacy. Data aggregation combines the data and brings fragments together, identification connects the aggregated data to an individual and makes the individual visible.[387] Thus, identification is one of the most central concepts of current privacy legislation, hooked to a phrase, ‘personally identifiable information’ (PII).[388] The first legislation to refer to the phrase was the Family Educational Rights and Privacy Act (FERPA).[389] Though

[387] Solove, D. J. (2004). *The digital person: Technology and privacy in the information age* (Vol. 1). NYU Press, at 1.
[388] Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *NYUL rev.*, *86*, 1814.
[389] 20 U.S.C. S. 1232g.

FERPA does not define the term PII explicitly, it is used for students' education records, as it is legislation to preserve students' privacy. FERPA defines education records as any information that is related to a student and stored by an educational institution.[390] Recognising the ambiguities of FERPA, i.e., it was necessary for the institution to store data to claim a breach of privacy, US Congress 1984 passed the Cable Communications Policy Act to define PII.[391] The 1984 Act prohibited any cable operator from collecting the PII of any person without their consent. The Act not only refers to PII explicitly but also rightly shifts focus from data aggregation to data collection. The Cable Act differs from FERPA, as the latter is only attracted to 'educational records' - an assemblage of information - whereas the former obligates the cable operator at the data collection stage.

Placing the said understanding in the context of this chapter, the collection of student data is a breach of privacy at the collection stage itself and not when it is aggregated with the Aadhaar database. Also, with technological advancements, the line between personally identified information and non-personal data is blurring. Many scholars have recognised the flawed notion of PII as now even non-personal data can be used to identify an individual, claiming anonymisation as a myth.[392] Further, due to technological advancements, today's non-personal data can be the future's PII.[393] Whether a particular piece of information can lead to the personal identification of an individual is dependent on the technology, the actors using the technology, processing abilities, and the information-sharing norms that permit the sharing and linking of data. Thus, the ability to identify an individual is not based on whether a piece is personal or non-personal data, it depends on context. Furthermore, as stipulated in the last chapter, a given context is an abstraction of the society, shaped by actors, the information types they collect, and the information-sharing norms they frame. This chapter outlines the abstract context, the actors operating in a school, and the information types they collect and aggregate. The next chapter devotes attention to the fourth and final element of Nissenbaum's theory, i.e., information-sharing norms.

[390] Id, 1232(g)(a)(4)(A)(i)-(ii).
[391] Pub. L. No. 98-549, 98 Stat. 2779 (1984).
[392] Ohm, P. (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA l. Rev.*, *57*, 1701.
[393] Acquisti, A., & Gross, R. (2009). Predicting social security numbers from public data. *Proceedings of the National academy of sciences*, *106*(27), 10975-10980.

CONCLUSION

Our personal and sensitive personal data is a category or a parameter in the digital infrastructures described in the chapter. Ian Hacking referred to the 'avalanche of numbers'[394], making populations, individual bodies, landscapes, and networks completely legible to data controllers or data fiduciaries. The advancement of recording technologies, statistical techniques or calculative strategies which produce aggregated datasets has an underlying intention and motivation - to provide welfare benefits or surveillance. The economic or political motive brings into existence digital artefacts and, with it, a host of stakeholders or intermediaries that cultivate our data.

The present chapter brings to light the techno-determinism of the government to design, develop and deploy biometric technologies and other artificial intelligence applications contributing to the construction of data infrastructures. The chapter theorises the social, economic, and political complexities behind the data practices embedded in the education stack, through Aadhaar. This is vital to highlight as emerging neoliberal dynamics of the economy make it imperative to (re)conceptualise informational and decisional privacy in a paradigm where data is embodied, situated, and networked.

Today, the most striking aspect of schools is the ubiquitous nature of surveillance conducted in within them. It has been made possible due to the variety of networked infrastructure and technologies being used. The schools have witnessed growth in deploying AI-based technologies in the last decade. The state-sanctioned deployment with the launch of the NEP as discussed above, pushes the school to adopt emerging technology systems. However, post-COVID-19 pandemic in 2020, there was an influx of online education platforms due to schools shifting to digital. It was an opportunity for private players to push technology to the government and capture children's data that was largely untapped until then. The government ties up with private players to not only deploy the technology but also create an architectural design for the development of the technology. Sharing Aadhaar information with private players, mandating schools to centralise education records, and asking institutions to share live information with the state's command and control centre are all acts that the Economist dubbed as a '*Coronopticon*'.[395]

[394] Hacking, I. (2015). Biopower and the avalanche of printed numbers. *Biopower: Foucault and beyond*, *65*.
[395] The Economist, *Creating the Coronopticon*, March 28, 2020, 17-20.

The quantity of data that the servers of the respective platforms can collect could range from name, student's school, student's device details like network and internet connection, date and time, content viewed and shared on the platform, logins, chats, lecture recording etc. The traditional classrooms without technology will be a distant dream as the new schools include surveillance through CCTV or biometric fingerprinting or GPS and personalised learning systems. The perpetual surveillance through such networks is compounded by the fact that children do not have the right to consent and thus are acquiesced to constant monitoring in exchange for their education. In this sense, they lose the right to autonomy and control of their information in the hands of corporate giants. Furthermore, in cases of technology, whether facial recognition or Aadhaar, services are often outsourced to third-party vendors (like enrolment agencies introducers etc.), which raises questions like the amount of data shared with the third-party vendor, storage duration, whether the data shared with the third party is used for profiling, targeted advertising, etc. Such opaque technology systems with inherent biases and zero algorithmic accountability (both factors discussed in subsequent chapters in detail) pose an intrinsic danger to informational and decisional privacy. In an information age, data does not sit in silos, and the education stack assumes that everything can be a potential data source within a particular temporality. Thus, the design and development of the education stack itself endanger the core constitutionally recognised fundamental rights of privacy. By introducing presenceless (via unique digital biometric identity) layers into the education stack, that contributes to efficiency in education governance. Still, it comes at the cost of privacy, which is being commodified.

To appreciate the impact of technologies in a given social sector, like education, the heterogeneity of that particular sector must be understood. The chapter starts by laying out the practices typical in an Indian school that form part of everyday life. It shows the diversification of the Indian school sector due to underlying heterogeneity in terms of wage distribution & income levels, identity formation and peer relationships based on caste, class, educational credentials, etc. Understanding heterogeneity in terms of the 'practices' in a school brings forth what *Nissenbaum* terms as 'context'. Although viewed as an isolated materiality, technology has an interactional social component when interacting with a particular contextual setting. Thus, technology should be understood in relation to the physical and social geography, i.e. in relation to the people, things and relationships within which it is entangled.[396]

[396] Taylor, A. S., Lindley, S., Regan, T., Sweeney, D., Vlachokyriakos, V., Grainger, L., & Lingel, J. (2015, April). Data-in-place: Thinking through the relations between data and community. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 2863-2872).

According to *Nissenbaum's* theory, two informational norms are key, i.e., *appropriateness* and *distribution*. While appropriateness refers to what kind of individual information is fitting to reveal in a given context, distribution refers to the movement of information across the context. The theory of contextual integrity claims that if one of the informational norms is violated, that would give rise to privacy being transgressed. The discussion of context shows how information related to class, caste, sexual orientation, religion, and place of birth is key to children's identity formation. It is not appropriate to reveal student information and if revealed should have sufficient safeguards to maintain anonymity. But the emergence of Aadhaar has led to collection of every single data point about an individual which when aggregated leads to total surveyability. Along with-it various government schemes, learning and management boards in schools and the underlying economic motivations of private players, have led to the breach of both appropriateness and distribution principle, leading to transgression of privacy.

The chapter discusses three of the four parameters of Nissenbaum's theory of contextual integrity, i.e., context, actors, and attributes/information types. The next chapter discusses the fourth parameter i.e., transmission principles. Transmission principles in Aadhaar and an advanced AI technology are fundamentally different. The chapter above discussed Aadhaar as it is a central repository that acts as a database for various AI technologies. Also, Aadhaar captures sensitive personal details of students without effective consent that breach privacy of students. But AI technologies being the central theme of the thesis requires dedicated attention as the transmission or distribution of data within them is unique. The next chapter uses the fourth parameter of Nissenbaum's theory and shifts attention from 'practices' to the materiality of AI technologies. Though the materiality keeps changing with each technology, the practices of an Indian school broadly remain the same. While the fourth chapter discusses Aadhaar as it unleashes different kinds of actors and information types, the fifth chapter lays importance to the inner functioning of a technology that are largely opaque. It will demonstrate that an AI technology is technically different from Aadhaar but raises issues of a similar nature in terms of privacy harms.

FIFTH CHAPTER

APPLYING AI/ML LIFECYCLE TO AN INDIAN SCHOOL

Discussing only Aadhaar in the thesis could have brought certain limitations. This is because Aadhaar does not squarely fit within the meaning of Artificial Intelligence. In light of a common consensus on a global definition of Artificial Intelligence, the recently conceptualised EU AI act defines AI as '*Artificial intelligence system' means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.* Annex 1 here means statistical techniques including Machine Learning, supervised or unsupervised. Aadhaar is a database that stores biometric data and uses a separate machine to authenticate or verify individual identity. It is different from technologies such as facial recognition enabled CCTV cameras, emotion recognition technologies, or machine used to predict dropout. Such technologies pose greater danger than Aadhaar and needs a separate analysis. While Aadhaar enables the previous chapter to advance Nissenbaum's contextual integrity framework, the discussion of the above-mentioned AI based technologies will show that the actors, attributes, transmission principles and the context evolve with each technology. Thus, the nature of harms caused, and the privacy lost is unique in any given technological context.

Apart from the 'practices', this chapter asserts that the '*materiality*' of the technology, i.e., what technology constitutes and how technology operates, also shapes an individual's privacy. **Part A** of the chapter discusses the fourth element of *Nissenbaum's* theory and sub-part of information flows, i.e., Transmission principles. Dissecting the transmission principles contribution to the thesis in three ways: a) Typifies how data is collected, annotated, processed, and trained, b) Introduces actors apart from the ones shown by way of Aadhaar case-study and c) provides a contextual study of what human choices lead to privacy harms.

This chapter will show how information is revealed at each stage of the AI/ML lifecycle without the knowledge of the data subject and distributed by actors at play to serve their objectives. First, **Part A** explains how an AI technology operates as it is aiding our understanding of its transmission principles. Further, **Part B** uses the AI/ML lifecycle to demonstrate how privacy gets lost at each of the stages. Upon reading Part, A and B, it will be concluded that appropriateness and

distribution is breached at each stage of the AI/ML lifecycle, thus breaching Nissenbaum's theory. The chapter now begins with understanding AI technology and how privacy is lost at each of the stages defined in the previous chapters, when deployed in the school context.

The meaning of Artificial Intelligence can be traced back to Alan Turing, a British mathematician, who in 1949 pitched the idea of bringing computing abilities within the realm of human intellect.[397] Through the Turing Test or the imitation game, Turing initiates a symbiotic relationship between human intelligence and computing abilities. The test questioned a computer's ability to pass behavioural intelligence. Despite scholars considering the Turing test as a pioneer in understanding AI (despite not using the term AI per se), it was prone to criticism. The Turing test depended on the 'behavioural standard of intelligence', which narrows the standard of intelligent behaviour to 'imitation', like humans. John McCarthy, who coined the term Artificial Intelligence, answers the criticism of the Turing test by broadening the definition of artificial intelligence. He defines it as:

> *"the science and engineering of making intelligent machines, especially intelligent computer programs… AI does not have to confine itself to methods that are biologically observable".*[398]

The definition provided by McCarthy moves beyond mere imitation to performing intelligent functions. He provides examples of intelligent functions, such as providing recommendations based on input data and moving to the tasks on which humans do not hold mastery. In the education context, a system providing recommendations on the likelihood of a child dropping out of school or grading a student based on their past education records can be called an AI system. In the said example, there are two fixed factors, i.e., education records as input data and the expected goal the system needs to achieve. There can be various desired goals specific to needs, ranging from recommendations, classification, or profiling. Based on the fixed factors a human input, the system autonomously performs the processing with no requirement of any external user. Humans only require feeding the input data and fixing the desired goal. However, computing abilities have advanced to a level where if the system detects any change in the environment, i.e.,

[397] Grudin, J. (2006). Turing maturing: the separation of artificial intelligence and human-computer interaction. *Interactions*, *13*(5), 54-57.
[398] McCarthy, J. (2004). What is artificial intelligence? *URL: http://www-formal. Stanford. edu/jmc/whatisai. Html*. Also Read, McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A proposal for the Dartmouth summer research project on artificial intelligence, august 31, 1955. *AI magazine*, *27*(4), 12-12.

changes in the 'fixed factors', the system autonomously perceives the change, reacts to the variation and achieves the set goals. The advanced stage is when the system becomes fully autonomous, and there is no need for interaction with human agents. If, in case, the desired outcome is not satisfactory, the input data is further developed and fed into the system. It creates a loop of improving the system by feeding its data hunger. Though the algorithm makers know and document the fixed factors at this stage, the processing is unknown to the public.

Opacity is at the heart of AI or intelligent computational agents by their design. Opacity is also one of the primary reasons scholars demand accountabilities from an artificial intelligence system to safeguard individuals' privacy rights.[399] Often, the reason for such opacity is located in the system's proprietariness, intentional corporate or institutional actions, or coding, a specialist skill known to few. The thesis accepts the reasons behind the system's opacity but emphasises opening the black box and understanding the machine learning lifecycle and the underlying data practices.

PART A: TRANSMISSION PRINCIPLES - THE 'MATERIALITY' OF THE TECHNOLOGY

Before we discuss how breach of privacy occurs because of AI technology's usage, it is essential to examine how data transmits i.e., how data is created, shaped, aggregated, structured and fed into a system. By paying attention to several 'data practices' that constitute an AI's lifecycle, we can provide a taxonomy of potential harms and benefits that run the risk of breaching or safeguarding the right to privacy, respectively. It is also essential to lay down the stages of the AI/ML lifecycle because several authors have discussed it as a singular process of input and output data. For Example, Barocas and Selbst identify three stages of the lifecycle defining the 'Target variables' and 'Class labels',[400] Training data by labelling it and feature selection.[401] To understand the process in a better manner, the following part provides a rich breakdown of AI technology's lifecycle. The lifecycle illustrated below shows data transmission across each stage and the informational norms amongst which data gets 'cooked'. Lehr and Ohm classify the

[399] Marda, V. (2018). Artificial intelligence policy in India: a framework for engaging the limits of data-driven decision-making. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133), 20180087.
[400] Authors define target variables as the outcomes of interest based on specific needs. And class labels divide all possible values of the target variable into mutually exclusive categories.
[401] Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *Calif. L. Rev.*, *104*, 671.

lifecycle into eight distinct parts: problem definition, data collection, data cleaning, summary statistics review, data partitioning, model selection, model training, and model deployment.[402] The authors divide the eight stages into two parts, i.e. '*playing with the data*, which involves the first seven steps, and the '*running model*', which involves the last part. However, the thesis claims that such bifurcation subsumes the design (where data is being gathered and fed into the system) and development stage (where the data is getting processed). Thereby, though Lehr and Ohm open the black box to avoid complexity, it improperly assumes the stages where, on the one hand, humans 'play with data' and, on the other, the computer autonomously processes the data. The present section divides the stages mentioned above into three sections, Design, Development and Deployment.

1.1. DESIGN

The designing stage refers to building infrastructural abilities for an artificial intelligence system, like gathering required datasets, identifying data sources, hiring a professional workforce to identify problems and labelling datasets, building on existing datasets and expertise, and exploring partnerships for data sharing and interoperability.

1.1.1 PROBLEM DEFINITION

The first stage of the lifecycle is when relevant stakeholders think about and decide on the output variable, also called the target variable. As pointed out above, the output variable is one of the fixed factors necessary to be identified initially as it indicates the future course of action regarding required datasets. It is upon the stakeholders like product developers, data scientists or software engineers to determine the outcome variables. Output variables can be based on classification algorithms with binary indicators like Yes/No, Hot/Cold, Green/Red, Pedestrian/Cyclist etc. There can be multi-label classification algorithms where output variables are more than two. Apart from classification algorithms, some can produce ordinal outcomes, like First/Second/Third. As Lehr and Ohm state, the first step of problem definition is turning an abstract goal into a predictive goal.[403] For example., measuring the likelihood of a student dropping out of school is the government's policy objective. Accordingly, AI systems that predict such dropouts may fix a predictive goal, such as detecting the number of students scoring less than 50% marks. It is because students who get fewer marks might have fewer chances of getting a job, so they feel it is better to quit formalised schooling. At this stage, an abstract goal turns into a predictive goal.

[402] Supra note 392, pp. 672.
[403] Id., pp. 674.

Now is the time to turn a predictive goal into a specific, measurable output variable. Though every output cannot be measured quantifiable, stakeholders tend to collect datasets with close reasonable proxies.

1.1.2 DATA COLLECTION

Once the data scientist has fixed the outcome variable, the goal is to collect the corresponding datasets that can yield the required output. In education, the data types can relate to teaching and learning or academic management. Teaching and learning data can include students' exam results, admission data, levels of participation, audio or video recordings, time spent on tasks, admission data, and assignment records. Academic management data, which is more non-academic data, includes students' bank detail, Aadhaar ID number, and entitlement records like mid-day meals, uniforms, books, scholarships etc. The two primary sources of education data are students and their parents, who provide information to schools, and the government schemes for data collection. For instance, the Unified District Information System for Education (U-DISE) is a database which was set up under the Sarva Shiksha Abhiyan government scheme in 2001 and currently collects data from 15 lakh schools (government and private) up to the secondary stage of the school, managed by National University of Education Planning and Administration (NUEPA).[404] District-specific information is uploaded on the website on an annual basis. There are databases at the panchayat level (the local form of government), where education data is collected from each household annually and compiled in Village Education Registers. National Sample Survey of 2006, 2009 and 2014 and the Indian Census of 2001, 2011, and 2023 collect several educational indicators.

The data-gathering process is crucial; as scholars point out, the technology is as good as its data.[405] The datasets are input variables, one of the fixed factors contributing to achieving the intended output. Depending on the context, often, either the data is not available or is not in a structured format. In such conditions, the data has to be obtained by aggregating several data points spread across databases to create a dataset required for the system. Such a process in which the data or the input variable is obtained from unstructured input information is called '*feature selection*' or '*feature extraction*'.[406] Let us understand with an example of using an AI

[404] Gorur, R., & Dey, J. (2021). Making the user friendly: the ontological politics of digital data platforms. *Critical Studies in Education*, *62*(1), 67-81.
[405] Harry Surden, Machine Learning and Law, 89 WASH. L. REV. 87, 106 (2014).
[406] Huan Liu & Hiroshi Motoda, Feature Extraction, Construction and Selection: A Data Mining Perspective 3-5 (1998).

system for grading students in a school. In this case, the output variable predicts grades, based on which the input variables should be decided. In 2020, the UK education regulator, Ofqual, used three input variables for grading students at A Level, namely: historical grade distribution of schools from three previous years (2017-2019), the rank of students in its school per subject based on teacher's evaluation of their likely grade in the event the exam would have gone forward as planned (called as Centre Assessed Grade), and previous exam results of a student per subject.[407] The regulator, rather than going ahead with the input variables acting as individual datasets, could have extracted features from each dataset to make an aggregated separate dataset as a whole. Thus, it is the concerned stakeholder's choice to decide regarding the choice of datasets, whether to gather or merge and whether to maintain their quality.

1.1.3 DATA CLEANING

The last stage, before data is fed to the system for processing and where it is prepared for testing, training, and validation, is called data cleaning. The input variables are vetted at this stage for any missing or inaccurate values if present. If missing values are found, one option is to delete the entire variable with missing values or delete the particular missing value. Such deletion is dependent on the number of observations of a particular variable. If the dataset on a variable is sufficiently large, deleting one particular value might not hinder the outcome. Apart from the number of observations, another consideration should be the representation of the particular value that is being deleted. If the particular value or the variable is not represented well in the dataset, questions of representation and generalisability fall on the outcome produced by the system. In addition to missing values, data scientists need to identify and work with incorrect values. While viewing the dataset in a tabular form, the missing values are not hard to be located as the cells would be empty or filled with 'NA'. However, incorrect values are not visible and might appear legitimate. A value that might be so extreme that it is bound to be incorrect is utmost likely the easy way out for the data scientists. Once incorrect or missing values are identified, if the data scientist intends, they can trace back to the data source and impute it with the correct value or delete the entire value/variable.

Data annotation is a practice by which experts in a given field are hired to either label or tag a given input variable - photo, video, or an object. It is labelled or annotated manually to make the raw data comprehensive and of sufficient quality. In education, multiple things can be labelled,

[407] Kolkman, D. (2020). F** k the algorithm?: what the world can learn from the UK's A-level grading fiasco. *Impact of Social Sciences Blog*.

like a child's facial features, handwriting, grades, attendance sheet, assessments, study habits, and peer relationships. If multiple experts are unavailable, one expert teaches and trains a pool of human annotators who annotate input variables. Often, big tech organisations have their in-house data annotation team, some outsource the annotation stage to third-party players, and the rest depend on non-experts' annotation.[408] If a data scientist thinks there would be a need for regular data annotation, this stage can be fully automated. However, several challenges are associated with the data annotation stage, discussed in the next corresponding section.

1.2. DEVELOPMENT

The development stage is where once 'cooked' data is assessed, partitioned, tested, trained and selected to achieve the intended outcomes. If, at this stage, the model seems to be biased, faulty, incomplete, or risky, the makers go back to the designing stage, and the loop continues until the desired outcome is achieved. The development stage can also be called data processing and is divided into three parts: Data Partitioning, Model Selection and Model Training.

1.2.1. Data Partitioning

An analyst intends to run the machine learning system in an actual world environment for which it needs to run the system on the data most resembles the real world. Therefore, one cannot run the entire machine-learning algorithm on the initially collected data. Also, as we learnt from the designing stage, the data collected could be marred by the challenge of not being representative, or time gaps could have made the data redundant. Randomness in the datasets occurs due to several circumstances, like the messy context explained above, that act as a barrier to achieving generalisability.[409] The data partitioning method allows the analyst to gauge the randomness in the data by splitting or partitioning an entire dataset into two: a '*training dataset*' and a '*test dataset*'. During data partitioning, the machine is forced to learn the predictions from the training dataset and prove its accuracy and other performance parameters through the test dataset. It, however, does not signify that data partitioning is a panacea for all data problems. If the concern is randomness in data through the previous stages, then data partitioning results might prove helpful, as randomness would differ in training and test data. However, this process is useless if

[408] Wang, D., Prabhat, S., & Sambasivan, N. (2022, April). Whose AI Dream? In search of the aspiration in data annotation. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (pp. 1-16).
[409] Domingos, P. (2012). A few useful things to know about machine learning. *Communication of the ACM*, *55*(10), 78-87.

the dataset is non-representative of the natural world; training and test datasets are curated from the same initial dataset.

1.2.2. Model Selection

By this stage, the problem has been identified, and data has been collected, cleaned, labelled, and partitioned. Until this stage, the algorithm is not mentioned as data is being 'prepared' for processing. The prepared data is trained and tested on selected algorithms to produce outcomes of interest. So, the next question at hand is how algorithms should be chosen. The answer again lies in the context and subjectivity of the data scientist. Therefore, as Lehr and Ohm state, model selection could be a complicated task that depends on six considerations or 'contexts': a) Choice of the outcome variable, b) Ability to implement an "*asymmetric cost ratio*", c) Explainability, d) Overfitting potential, e) Tuning, and f) Resource Limitations.[410] Each context can potentially cause harm and breach of privacy, explaining each in the next section.[411]

1.2.3. Model Training

The data is gathered, labelled, and partitioned along with a chosen algorithm tuned with the training data. Now, it is time for the learning aspect of machine learning, where the algorithm is run on the training dataset and learns to make the final prediction by way of yielding output variables. Model training is not a disjunct task of running an algorithm once. Instead, it is a continuous and repeated exercise of running, tuning, validating, and selecting parameters. There is no clear or formal way of running an algorithm as the process vacillates across the abovesaid tasks. The first process is '*function optimisation*', meaning generating predictions - maximum or minimum - by running the algorithm on the training data concerning the assigned function or output. Additionally, optimising the model aids in choosing the hyperparameters for the model, allows transformation to the input variables, if any, and validates the algorithm's accuracy. Thus, function optimisation aids in tuning the algorithm, i.e., fitting the learning algorithm to the training dataset.

Another critical consideration that undergoes tuning is bias and variance error. Upon training the data, the model can yield errors broken down into Bias and Variance errors. A bias error occurs when the model makes assumptions to learn the output variable. Variance Error is the model's sensitivity to small fluctuations in the training dataset. Ideally, the model should produce similar

[410] Supra note 392, pp. 688.
[411] Infra, Part B.

predictions on all training datasets. Generally, linear algorithms are prone to high bias errors making them less flexible than Logistic Regression or Linear Regression algorithms. However, nonlinear algorithms, i.e., have high flexibility and variance, like Decision Trees or Support Vector Machines model. Thus, linear algorithms have high bias and low variance, whereas nonlinear algorithms have high and low bias, also known as the Bias-Variance tradeoff.

Tuning is not a one-time process as the model maker assesses each round, and accordingly, changes, as described above, are made to the model. Tuning does not offer a definitive solution; therefore, the model must be re-tuned, re-trained, and re-assessed. It brings into factor the choices that are made regarding assessment methods. Generally, the three primary metrics used for assessing the model are accuracy, precision and recall. Still, the choice of assessing the model on these metrics depends on the model maker's subjectivity.[412] Also, it is not necessary that the model is evaluated in alignment with the three stated metrics.

The last step under the model training stage, though not necessarily in order, is feature selection. Feature selection is choosing and narrowing down the input variables while re-tuning and assessing the model.[413] Feature selection is not an isolated step and might not even be required by each model maker and purely depends on each model's objective. It happens or should happen alongside tuning and assessment. As Lehr and Ohm state, primarily, feature selection defeats the idea of the "*curse of dimensionality*".[414] This phrase includes that when the makers intend to generalise the model, make the model less prone to bias and variance errors and provide representative data to the model, the input variables increase. Increasing the input variables exponentially increases the training data to cover all possible relationships between the input

[412] For instance, in the case of Amazon, the outcome of any evaluation contains a) An accuracy matrix on the overall success of the model, b) Visualisations to depict the accuracy of the model, helpful for interpretability purposes, c) Review of the advanced metrics like precision and recall to get a threshold score. Herein, precision measures the fractions of actual positives among those predictions that were true and false positives. And recall measures the fraction of actual positives among those predictions that truly belong to a particular class, i.e. true positives and false negatives. For more detail, see https://docs.aws.amazon.com/machine-learning/latest/dg/machinelearning-dg.pdf#evaluating_models, pp. 87-90.

[413] Feature selection is different from phrases like feature extraction, feature transformation, or feature construction, where primarily the input variables are gathered, collected and cooked. Feature selection is done if required based on running the algorithm repeatedly on training datasets.

[414] Friedman, J. H. (1997). On bias, variance, 0/1—loss, and the curse-of-dimensionality. *Data mining and knowledge discovery*, *1*(1), 55-77.; Guyon, I., & Elisseeff, A. (2003). An introduction to variable and feature selection. *Journal of machine learning research*, *3*(Mar), 1157-1182.

variables and reach a better outcome. The feature selection process should be done sequentially by pruning the input variable and then assessing the model results to validate the pruning.

1.3. DEPLOYMENT

Once the model is trained and validated, it can be deployed in the real world. It is the stage where the data scientists take a back seat as the model is designed and developed. It is now upon the project software engineers to deploy the system effectively and at scale. It is the stage where back-end data infrastructure comes into consideration, allowing smooth model implementation in a real-world environment. The data scientists are among the most critical stakeholders here, as their model is coming to fruition. A cross-cutting collaboration of teams from the Product Development, DevOps, and Data Scientist Teams is needed to deploy the model. The DevOps team provide the technical back-end infrastructure responsible for deploying the model. The team is also responsible for the stability and security of the whole process. Finally, the product managers are the ones who are responsible for providing the best user experience of the model through which the model attains its value. Thus, all three respective teams have a stake in the success of model deployment and its political, social, economic and legal considerations. Diverse responsibilities and needs across these teams can pose risks and challenges for model deployment. Though there are no stages of deploying an AI system, a few things are considered, like the model's ability to adapt to changing situations for which it was not explicitly trained and whether the model is user-friendly.

As the three overarching stages of the lifecycle show, AI technologies predictions are a labour of multiple human choices. Legal scholars fail to articulate or study such human choices due to the technicalities involved. Thus, Part C outlines the technical details, the underlying data work that leads to not only loss of control over personal information but also wrong predictions. The understanding attained through Part C can enable a better regulatory agenda to mitigate algorithmic privacy. The solutions need not be technical that meet the threshold of over or underfitting or meet the fairness criteria, rather legislative solutions which reduces the impact of each data practice on privacy.

PART B: LOSING PRIVACY AT EACH STAGE OF THE LIFECYCLE

Artificial intelligence systems are deployed to improve education and drive evidence-led policymaking. The evidence that leads to better education governance and policy outcomes

comes from the data fed and processed by such systems. Without accurate, timely, authentic and reliable data, AI systems are expendable. However, Kiri Wagstaff stresses that machine learning happens on isolated and narrowed benchmarked datasets today. His paper, more than criticism, asks the machine learning community for a self-introspection about whether there is any connection between 'machine learning research and the world of scientific inquiry.[415] Machine learning in today's world focuses more on algorithms and model development, using prepared datasets and their technicalities. It does not motivate questioning the interpretation of datasets, like whether the dataset is representative, how it was collected, who collected the data under which environment, what errors can creep in while collecting or using datasets and the impact of such errors. As recent scholarship aptly puts it, '*Everyone wants to do the model work, but not the data work*'; machine learning under-values data work, where errors creep in first, and not at the model development stage, which is most valued.[416] The recent data focus is also mostly on 'high-stake domains', like healthcare and fintech, which are deemed to involve safety and well-being. First, the present thesis looks at the education sector and the data it generates as sensitive and personal. It argues for its determination as a high-stake domain if there is any definition to which it can be attributed. Second, there is no comprehensive scholarship in the Indian educational context that evaluates the model. The data work through the lens of individual privacy, and thereby Part B is an attempt to close this gap.

Part B explores the data processes and practices undertaken in an Indian educational setting and shows how such 'practices' affect individuals' privacy. In this context, privacy is evaluated from the lens of varied harms emanating from the 'practices', such as discrimination, inaccuracy, exclusion, bias, and explainability. This chapter recalibrates the stages mentioned in the previous chapter to explore the harms associated with each stage. While examining and recalibrating the distinct stages of machine learning, the chapter argues that each stage has downstream impacts culminating in a breach of individuals' privacy.

2.1. PROBLEM IDENTIFICATION

While defining the output variable, the stakeholders intend to turn amorphous output variables into measurable outcomes. Selecting output variables can be quickly addressed if it can be

[415]Wagstaff, K. (2012). Machine learning that matters. *arXiv preprint arXiv:1206.4656*.
[416] Sambasivan, N., Kapania, S., Highfill, H., Akrong, D., Paritosh, P., & Aroyo, L. M. (2021, May). *"Everyone wants to do the model work, not the data work": Data Cascades in High-Stakes AI*. In *proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-15).

formalised into 'class labels' (input variables) which rely on binary classifications. However, in some instances, achieving the desired output variable is chaotic as it involves the creation of new input variables. These are the situations where output and input variables cannot be directly measured or quantified. For example., in the case of the likelihood of a student dropping out of school, how would someone measure 'dropping out? There can be multiple factors behind dropping out, like lack of funds, the distance between house and school, improper infrastructure available in a particular geographic location, or disinterest in studies. Even more challenging is an AI system predicting the grades of a student (abstract goal) based on past performance (predictive goal). Past performance can again be linked to multiple causes, like the quality of teachers and school infrastructure to the likeness of a particular subject. Such factors are also part of an array of parameters linked to a student's grades or likelihood of dropping out. It is impossible to reasonably convert each attribute into a measurable format because each school and teacher has its way of constructing the behaviour or marking a child's performance. Subjecting the behaviour or performance of a child to a narrow set of variables can be a nonarbitrary decision pervading discrimination.

Lehr and Ohm state that data scientists choose by considering their subjective knowledge, technical implications, and resource limitations for output variables that can be measured.[417] First, a data scientist steeped in the educational context, based on their subjective knowledge, might have a good reason to say that the past marks of a student should be measured for predicting grades. Second, technically, different algorithms work differently with different output variable forms, so a data scientist can be prompted to choose a particular output variable, not necessarily the one originally intended. Lastly, there can be resource constraints regarding the budget of an actor making an AI system that calls for hiring a workforce with less technical and institutional knowledge or some output variables that can be easy and cheap to measure, inducing the actor to choose them. Problem identification, i.e., an AI system's intended goal or outcome, originates from various economic, social, political, and cultural constraints. Thus, through this subjective process, problem identification might systemically disadvantage certain marginalised sections of the population. In order to address this concern, the legislation should mandate the data controller to document the reasons behind mandating the deployment of such a technology. Such reasons can then be adjudged upon by the courts against the necessity and proportionality test.

[417] Supra note 392, p. 675.

2.2. DATA COLLECTION

Data gathering poses threefold challenges identified by Lehr and Ohm that can cause concerns regarding privacy harms: when is data enough, faithful measurement and generalisability.[418] Machine Learning algorithms thrive on data and are known to produce accurate results as the "number of observations in a dataset grows toward infinity", for which many datasets are required.[419] No regulation defines the benchmark for minimum data collection as it happens according to the context and choices made by the stakeholders. For example., an Artificial Intelligence system detecting the behaviour from students' faces in a classroom has no benchmark for how many types of behaviours the model should be trained. Nowadays, CCTV cameras are embedded with facial recognition systems, deployed in classrooms where each image is broken down into 'biometric numerical representations' from which a system analyses a student's behaviour, i.e., whether it is happy, sad, attentive, sleepy, etc. Thus, a large set of facial images are gathered and merged for each emotion to train the system. '*When is data enough*' also brings a question of '*What data is enough*' as, in the earlier example, a student might show different behaviours to stimuli. Each student does not need to behave the same way a model is trained. Thus, dataset's quantity and quality can create bias and discrimination.

The next challenge is to ensure that variables not only measure what they indicate on their face but what data scientists want them to measure or for what they were sought in the first place (a latent construct) - called faithful measurement. Let us understand the example above of designing facial recognition systems for classrooms. During the last two years, we saw a rise in ed-tech platforms designing tools that provide AI-based proctoring services[420] and facial coding systems measuring students' cognitive and emotional responses.[421] For the variables, such platforms collect data points like students' facial expressions, eyelid, lip or cheek movements, voice and any change in its inflexion, and gestures to flag output variables like classroom engagement, behaviour, and learning patterns. On the face, though the input variables can be validly measured, it is likely not a 'faithful measurement' when its underlying latent construct is understood. The underlying construct of such input variables is that these are unreliable data points because

[418] Ibid, pp. 679.
[419] Id, pp. 678.
[420] Motwani, S., Nagpal, C., Motwani, M., Nagdev, N., & Yeole, A. (2021). AI-Based Proctoring System for Online Tests. *Available at SSRN 3866446*. Also refer to Mettl website which provides the software to top Indian institutes. https://mettl.com/en-gb/online-remote-proctoring?utm_source=direct&utm_medium=website&. .
[421] For instance, affect lab is providing facial recognition and emotion mapping services to institutes. For details, refer to, https://affectlab.io./.

research has shown patterns of muscle changes among children and young adults, making the measurement egregious.[422] One of the research teams in Maharashtra at Leadership for Equity (LFE), in partnership with Flame University's professors, is developing a tool to map Social and Emotional Learning competencies (SEL) in Maharashtra based on the CASEL framework (*Collaborative for Academic, Social and Emotional Learning framework*) - a widely reputed framework to evaluate SEL in local contexts. The team also highlights the challenge of choosing and collecting data for SEL competencies as it is difficult to define and quantify them.[423] Also, competencies vary with the age, gender, and culture of the student. To measure anger when someone disagrees with you, asking children how they respond when teased or provoked might yield completely different responses. While collecting data, the answers to two similar questions might be different. In contrast, in the former question, the emotion is already mentioned, the latter gives a chance to the student to describe the emotion. Thus, it is tough for an AI system to be designed through data that accounts for living contexts and cultural realities resulting in '*unfaithful measurement*'.

The third challenge during the data collection stage is to frame datasets so that once the algorithm is trained, it produces accurate predictions once deployed on different data, called Generalisability. One of the challenges in data collection is its non-representativeness. The data collected should represent the population on whom it will eventually be deployed; for instance, in the Indian state of Maharashtra, SARAL software stores all the administrative and academic data of all schools and their students. It was reported that the data of over 78.643 students studying in classes IX and X is missing from the system.[424] Data processing depends on drawing relationships between several variables and predicting the outcome. Similarly, almost a decade ago, the University Grants Commission, the parent body of all higher educational institutions, whether public or private, reported to the Parliament about missing data on universities.[425] UGC

[422] Barrett, L. F., Adolphs, R., Marsella, S., Martinez, A. M., & Pollak, S. D. (2019). Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements. *Psychological science in the public interest*, *20*(1), 1-68.
[423] K. Sharvari, "Using Data to Improve how social-emotional learning is measured", The Bastion, May 26, 2022. Available at, https://thebastion.co.in/politics-and/education/using-data-to-improve-how-social-emotional-learning-is-measured/.
[424]G.S. Swati, Data of 78,000 Maharashtra students goes missing, ToI, Jun 1, 2021. Available at, https://timesofindia.indiatimes.com/home/education/news/data-of-78000-maharashtra-students-goes-missing/articleshow/83128536.cms.
[425] J. Isha, "Incomplete data hits University Grants Commission", ToI, Mar 25, 2011. Available at, https://timesofindia.indiatimes.com/city/lucknow/incomplete-data-hits-university-grants-commission/articleshow/7784223.cms.

attributed the 'missingness' to incomplete databases, digitally unequipped, and lack of staff. Another critical parameter was the uneven format of universities concerning UGC; the former, for example, did not collect the gender-wise data the latter requested. Not collecting diverse data sets and not arranging them on gender, age group, disability, or other parameters can result in minimum interrelationships between data variables. Thus, any AI model relying on UGC-level datasets, which are inherently narrowed, inaccurate, and biased, might be potentially inaccurate and biased.

Also, often the systems take a long time before they are deployed, which means the data measurement at the data collection and the deployment stage differs. Due to the time lag, sometimes the make-up of the population on which it is supposed to be deployed also changes. However, AI-use cases in schools remain unaffected due to the time gaps, provided that the random data sampling is representative of the students. Despite the time gap argument not holding water, representation in the dataset should be varied so that inclusivity remains. Take, for instance, the similar example of using a facial recognition system to detect students' behaviours in which even data of 50,000 students across schools of a particular district cannot be generalisable. School behaviours vary with age, gender, socio-economic background, classroom environment, teacher-student relations, and students' confidence. Also, while data is being gathered in schools, the data collector must build rapport with the students by understanding their sensitivities to give definitive answers to similar-looking questions. Otherwise, models working on one dataset might yield different results when treated on a similar-looking, different dataset. Thus, deciding on students' engagement in the class by relying on the outcome of an AI system is potentially discriminatory and might prove harmful to the students.

In most states, though there is a hierarchy for data collection from schools, it is marred with overburdening and unskilled workers, explained in detail in the following section. At the cluster level, the teachers collect the data from the Zonal Education Officers and submit it to the UDISE portal, where the Chief Education Officer examines it. The UDISE data of each school is also evaluated at the central level by the Ministry of Human Resources Development - now the Ministry of Education - and used for project approval and disbursal of funds.[426]However, mere data collection is impractical if the context behind its collection, i.e., who is collecting and how it is being

[426] Greater Kashmir, “In J&K government schools, flawed UDISE data hampers infrastructure upgradation”, 19th May 2018. Available at, https://www.greaterkashmir.com/kashmir/in-jk-govt-schools-flawed-udise-data-hampers-infrastructure-upgradation.

collected, is not examined. The explanation under the next stage is an attempt to highlight the 'messy context' in which data is collected and prepared and who are the stakeholders behind the process.

Professor Kate Crawford has stated that data is collected randomly and unequally across geographies, covering people of varied lifestyles, often ignoring those who are comparatively less '*datafied*' than the general population - referring to such processes as 'dark zones' or 'shadows'.[427] In the education context, the rural school students or the states with digital infrastructural constraints have been historically disadvantaged as they did not participate in the initial data collection activities. Now when the technology - that has been built using '*privileged schools and students' data*' is deployed, not only would the quality of the former students or states below, but also the quantity in terms of overall representation would be dismal. If the model were to rely on such unrepresentative data to allocate resources and implement education policies, it would not only discriminate but also underserve the already ailing schools. Such models provide generalisable findings, often overlooking the statistical bias prevalent in the datasets.

In order to address such concerns, the legislation should mandate the data controller to document the data collected to train the technology and make it available for auditing purposes. Such a transparent obligation would aid data subjects to address their rights effectively and understand how particular technology operates and make decisions about them.

2.3. DATA CLEANING

There are various reasons for missing or inaccurate values in a particular dataset. It can be the fault of the data collector not gathering the information in a correct format, the provider of information giving faulty information or opting out from giving information, handwritten information not being legible, data collection not trained or skilled enough to collect information, the provider being illiterate or mere accidentally deletion of data. In this messy context, data is gathered and requires data cleaning, without which the algorithm's inaccuracy can result in individual harm. It is essential to define and examine the messy context for two crucial reasons: how a breach of the right to privacy occurs and the attribution of liability in case it occurs. Outlining messy context means the stakeholders who collect the data, the environment in which they collect and prepare the data, the incentives they get for such preparation, or what kind of data gets prepared. Each

[427] Kate Crawford, Think Again: Big Data, FOREIGN POL'Y (May 10, 2013).

context continuously evolves, having its own set of preparation, varied stakeholders and incentives, and thus, it is difficult to lay down an overarching structure.

In the education context, teachers are not only being surveilled, as seen in the third chapter but are also the primary data collectors. In addition to their academic duties of preparing lesson plans, invigilation or designing curriculum, they are burdened with non-academic duties of collecting information like attendance, students' exam results, and enrolment data. Such non-administrative work has been attributed names by the teacher's like '*record-keeping*', '*clerical*', and '*non-academic*'. Teachers must collect such information and prepare the data by organising, verifying, and validating the data entry. Data preparation regularly faces challenges of parents and students not being literate enough to fill the forms accurately, the low competence of the staff, regular interruptions by other academic activities disrupting the flow of data preparation, and being overburdened with managing large datasets due to resource constraints and other procedural inefficiencies.[428] Additionally, it has been well reported that teachers often misreport the data to show the school in good light. For instance, in Nagaland, school authorities were found conjuring numbers concerning several students in the class, the quality of school infrastructure and the provisioning of Mid-Day meals.[429] Floating high enrolment numbers are directly proportional to getting higher grants by the government, which acts as an incentive to misreport the facts. Apart from the incentives, some information cannot be translated into binary data of Yes/No, like 'quality of infrastructure'. It is contingent upon teachers' subjective knowledge and interest to report on how good the toilets are or whether the meals taste good. Thus, though the teachers might collect the entire data, it is prone to incorrect values, making data cleaning imperative.

In addition to the teachers, various government schemes are meant to collect education data, as pointed out above. For instance, U-DISE is meant to unlock information in the education sector and provide credible evidence to the government for policymaking. However, the data collected under government schemes must be more bereft of methodological anomalies and administrative mismanagement. The feast of data sources often provides varied and contradictory evidence on indicators like learning quality index, student retention levels, dropout percentage and quality of

[428] D. Vincy, "*Why Delhi's government school teachers feel they are not doing the job they were hired for"*, The Print, 25th June, 2019, Available at, https://theprint.in/opinion/why-delhis-government-school-teachers-feel-they-are-not-doing-the-job-they-were-hired-for/254061/.
[429] M. Diepeu, Strengthening Data Quality: A step to resolve education debacle, Nagaland Post, July 7, 2021. Available at https://www.nagalandpost.com/index.php/strengthening-data-quality-a-step-to-resolve-edn-debacle/.

teachers.[430] The discrepancies between the two datasets occur due to varied methodologies. For instance, the National Sample Survey questions, '*How many children are currently attending school*', and the Census notes the '*admission status in educational institutions*. The question that demands an answer is whether the AI system designed to gauge dropout rates should rely on NSS or census data. Furthermore, education being a state subject, each state government collects data in different formats, whereas the Central government uses their formats. It raises the issue of dataset congruency, i.e., data interoperability.

Apart from methodological discrepancies, administrative mismanagement leads to patchy policymaking and inadequate protection of rights. One includes resource constraints due to which only five per cent of the data in a particular district are randomly sampled and validated for accuracy. Mathematically, it means that data for two districts per state is randomly sampled and validated. Such data cannot be cross-checked across databases because each dataset collects data across age groups and time gaps.[431] Thus, U-DISE data, regarded as the most comprehensive school-level data annually updated, cannot be said to be accurate and reliable. An AI system designed to surveil teachers for their performance would generally record their absenteeism, employment status and the total number of teachers in a school. Though the data parameters sound statistical, however, are complex to record and might generate missing and incomplete values. U-DISE collects state-wise information on teachers, though in different formats. Some DISE state formats collect data only on permanent and contract teachers but hire fixed-term, para, and voluntary teachers. An AI system relying on DISE data will view all teachers as the same, showing significant absenteeism rates of voluntary or fixed-term teachers without understanding the contractual details. The need for more resources for data cleaning raises questions about the choice of datasets for an AI system and the system's credibility.

Another challenge, though it creeps in at the data collection stage, has a trickle-down effect on the data cleaning stage too. For data collection of any AI system, if the tools used in the education context are questionnaires or semi-structured interviews, their language and sentence formation

[430] B. Kiran, "*Better Data can improve public education in India - Draft National Education Policy says it too"*, The Print, 19th June, 2019. Available at https://theprint.in/opinion/better-data-can-improve-public-education-in-india-draft-national-education-policy-says-it-too/251715/.
[431] Kiran Bhatty, "*The Numbers Game: How Well has it served the cause of Education?*", The Print, April 14, 2018. Available at https://www.epw.in/journal/2018/15/insight/numbers-game.html. Also read, Greater Kashmir, "*In J&K government schools, flawed UDISE data hampers infrastructure upgradation*", 19th May 2018. Available at https://www.greaterkashmir.com/kashmir/in-jk-govt-schools-flawed-udise-data-hampers-infrastructure-upgradation.

mode can also lead to missing or incomplete values. For instance, the team at Maharashtra schools collecting data on SEL had to reframe the statements as questions to get the specific answer intended. They found variations in the answers when asked in the form of statements as opposed to questions. They were prone to errors while recording the data manually, as they did not account for dialects in Maharashtrian schools, where Marathi was the majority-speaking language, not Hindi or English.[432]

Like data collection, data annotation in the education sector is also done by teachers, often trickling down to the students through assignments. Neither teachers' nor students' primary duty is to annotate data, nor can they be called expert data annotators. To understand it clearly, let us take an example of data annotation in a different context. In agriculture, an AI tool is made to make pest management efficient. For such purposes, pest management traps are deployed to scrutinise each trapped pest. Entomologists who understand the pests are called upon to see the trapped pest's image and label each part, i.e., wings, feathers, eyes etc. Due to the paucity of entomologists in the country, they train agriculture students to annotate if required.

Similarly, in the age of social media, human annotators manually label words that can be perceived as derogatory, abusive, or propelling hate speech. The education sector can be chaotic for data annotation as many variables are annotated. In the case of a facial recognition algorithm detecting children learning engagement, psychologists and education professionals might be needed. Even if both are involved, it might leave some room for errors due to contextualities involved, like which emotion corresponds to increased or decreased learning engagement. It should be labelled the same across classes, genders, age-group etc. If such correspondence between input variables is not clearly shown, biases and inaccuracies can creep in at the model training stage.

To some extent, the challenges with annotation are like the data collection stage: a) the Limited number of available experts, b) the challenge of understanding the 'messy context' by the non-experts, and c) the time-consuming process. Due to such challenges at the data collection and data annotation stage, the dataset preparation process gets biased. If such biased datasets are used for model training, the dataset's prejudice can make the entire system, at best, result in exclusion and at worst the system’s predictions breach student’s and teacher’s right to privacy.

[432] Supra 428, The Print.

Similar to the data collection stage, to address privacy concerns at the data cleaning stage, documentation and auditing is key. Further, teachers and student involvement in data annotation is useful but it needs a separate regulation discussed in the last chapter.

2.4. DATA PARTITIONING

During data partitioning, the descriptive statistics in a dataset are split to produce prescriptive statistics. However, while partitioning the data, analysts face the challenge of splitting them into training and testing. If most of the data is used as a training dataset, then the model has various data to learn predictions. But, if the test dataset is left with less data, it will give a poorer result on the generalisability of the data and whether the model can work on the data other than on which it is trained. Ian Witten explains that more data is needed for training to find a good classifier, and the testing dataset needs more data to obtain a reasonable error estimate. It leaves the question of whether to do a 50-50, 70-30 or 80-20 split, which is helpful for systems' prediction. Lehr and Ohm state two interrelated considerations that can guide the splitting choice but caution that such choices are subjective.[433] The first consideration is the size of the initial dataset. Suppose the initial dataset is large and representative enough. In that case, it is easy to split the datasets into training and test data as all would be provided with variables from which the model can learn. There is no set mathematical formula for splitting the datasets, but the dataset's quality and size should be considered. Firms have even seen the ratio going to 90-10, but it depends on the earlier stages of how data is defined, collected and cleaned and therefore the solutions of documentation and auditing highlighted above are key. It is important to note herein that a large dataset can also have the majority of data points that are of no use and only a few rare things asked to be predicted by the model - this property is known as a 'long *tail*' or '*heavy tail*'.[434] One feature of the long tail is that the model has been fed massive datasets and is required to omit most of the data while processing narrower data to predict rare events. In cases of 'long *tail*', it is to the analyst's subjectivity to split the datasets and train their algorithm for the rare outcomes of interest. This subjectivity is the second consideration formulated by Lehr and Ohm.[435]

It is upon the domain expertise and subjectivity of the data scientist to perform a balancing exercise of evaluating the algorithm's predictive behaviour on the training dataset versus the ability of the algorithm to predict on an unseen test dataset. If the data scientist believes the

[433] Supra note 392, pp. 686.
[434] Ibid, pp. 687.
[435] Id.

outcome variable, she wants to achieve is not dynamic and would not dramatically change, then the training dataset's composition could be more significant. But training data on a larger the dataset would be useless if the domain or the outcome variable is prone to dynamic changes. In the latter case, the model's performance can be analysed on the test data if such data capture real-world dynamism.

2.5. MODEL SELECTION

The interrelationship between data and the algorithm comes into light at the model selection stage. Based on the input variable collected and prepared and the choice of the intended output variable, the algorithm on which data shall be processed is chosen. As discussed above, the model selection involves a few contextual considerations that can potentially lead to harm, thus demanding an understanding.

The first consideration is the choice of the kind of outcome variable. Depending upon the outcome, it limits the choice of the type of algorithm. It is because the algorithms can provide only specific outputs like ordinal outcomes or only deal with mathematical calculations or predictions related to classifying objects.[436] So fewer algorithms exist if the output variable, which is decided at the first stage of problem identification, requires ordinal outcomes.[437] Similarly, neural networks, another commonly applied machine learning algorithm that can process several interrelated aspects of data by analysing training examples, can produce binary outputs and classifiers.[438]

The next consideration of the output variable is implementing an "*asymmetric cost ratio*" (the difference between profit and loss). In the AI system, the profit is an accurate prediction, whereas inaccuracy leads to a loss. Despite how well one performs the mentioned stages, an AI system is prone to errors or inaccurate predictions. In the case of a binary output (or two-class case), accurate predictions are known as True Positives and True Negatives. Errors are known as false positives (when the outcome is 'yes' when it should not be) or false negatives (when the outcome is predicted as no when it should have been positive). For instance, a machine learning algorithm determines each cow's days as '*in estrus*' or '*in heat*'. The system predicted that cows were '*never in estrus*'. What was needed here was the prediction of the 'in estrus' rather than the 'never in

[436] Hardesty, L. (2017). Explained: neural networks. *MIT News*, *14*.
[437] Breiman, L. (2001). Random forests. *Machine learning*, *45*(1), 5-32.
[438] Once neural networks run on labeled data which is an input variable, it is capable of producing binary outputs using the process called as logistic regression.

estrus' situation. Both the said predictions associate with them two different kinds of costs.[439] The stakeholders' intention of the desired output determines if she wants to implement an asymmetric cost ratio and how. For instance, where the likelihood of arrestees committing domestic violence was predicted, more importance was paid to the prediction that arrestees would not commit domestic violence when they did, eventually implementing asymmetric costs through a random forest algorithm.[440] So different output variables leading to different kinds of errors push for different choices for model selection.

The model selection can also depend on the interpretability and explainability requirements of the data scientist, which is the third consideration. While explainability refers to understanding the causation of the effects of AI, interpretability measures the degree to which one can understand the cause. Both concepts help to monitor and make AI accountable. Explainability is crucial to transparency as the systems are considered 'black box'.[441] However, the type of algorithm chosen makes the system a black box. For example, a random forest is considered a simpler model than neural networks, making the latter more complex, thus, less explainable.

Highly well-trained data might lead to poor and harmful outcomes as they are not generalisable to all kinds of data. When the model is being trained continuously on the same dataset, it begins to learn the noise and fluctuations of the training data. In technical terms, it is known as '*Overfitting*' - modelling the training data too well - which is also the fourth consideration. Specific algorithms are flexible enough to approximate the output variable depending on the input. One such algorithm is the Random Forest decision trees algorithm that, due to being 'nonparametric' and 'non-linear', has more flexibility to learn about output from the training data - learning its flaws - negatively impacting the model. While plotting the errors on the graph, if the model's performance on training data goes down, generalisability also decreases, meaning that the model is learning irrelevant noise, making it overfitted. Such graph plotting can also produce the 'sweet spot' just before the error on the test dataset increases. This point would mean that the model has good skills in both training and test dataset.

---

[439] Witten, I. H., Frank, E., & Hall, M. A. (2005). Credibility: Evaluating what's been learned. *Data mining: Practical machine learning tools and techniques*, 143-186. pp. 180.
[440] Berk, R. A., Sorenson, S. B., & Barnes, G. (2016). Forecasting domestic violence: A machine learning approach to help inform arraignment decisions. *Journal of empirical legal studies*, *13*(1), 94-115.
[441] Adadi, A., & Berrada, M. (2018). Peeking inside the black box: a survey on explainable artificial intelligence (XAI). *IEEE access*, *6*, 138-160.

While the model is being trained on historical datasets, and before a specific algorithm is chosen, it reveals certain parameters that are key to ML algorithms. Parameters refer to values that define the problem for which the model is being designed. However, not all parameters can be estimated from the data. For such purposes, model hyperparameters are added - external and manually specified by the maker, to discover the parameters that can offer the best predictions. Adding hyperparameters and discovering parameters is called 'tuning' the algorithm. The tuning process can bring biases for two reasons: a) More hyperparameters, slower the tuning process, which can act as a disincentive for adding all the required hyperparameters, and b) Different algorithms have different important hyperparameters to focus upon,[442] bringing the decision of ML practitioners under scrutiny that why a particular model was chosen.

All the challenges mentioned above are mathematical considerations that require casting a legal eye. But, there is one significant practical barrier for choosing a barrier, also the last consideration, i.e. resource limitations. Regarding resource limitations, there is a '*cost-benefit trade-off*' wherein the model makers can argue in favour of higher rates of inaccuracies in exchange for easily accessible information. Model makers may be incentivised to operate disproportionately, provided the model-making is cost-effective. Obtaining information is costly, especially for varied datasets generalisable to the entire population. Also, ML algorithms require time, processing energy, and memory capacity to run, increasing complexity.[443] When there is a large dataset, one might choose a specific algorithm that processes the data faster. Similarly, stakeholders might be different in choosing the type of algorithm depending upon the available funds - between government and private actors and between bigger and smaller private players. Ideally, the model should be trained on several algorithms to determine which algorithm provides the best prediction. However, it is a time-consuming process. Such considerations are made solely by the maker in an opaque format. To address such concern, data subjects should be given a right to ask for an explanation behind a designing and developing reasons of a given technology. Such a right can provide an avenue of grievance redressal by seeking explanations from a data controller in a clear, concise, and interpretable way.

[442] For instance, Logistic Regression does not have any hyperparameters to tune whereas in Bagged decision trees algorithm the most important parameter is the number of trees.

[443] G. Lauryn, G.C.J, L. Peter, S. Kent et al., How to select algorithms for Azure Machine Learning. Available at https://docs.microsoft.com/en-us/azure/machine-learning/how-to-select-algorithms. How to select algorithms for Azure Machine Learning, 3rd January 2022. It compares several ML algorithms on the basis of their training times and accuracy. Training time and accuracy often accompany each other.

2.6. MODEL TRAINING

The first step in model training is function optimisation, as discussed in Part A, which recommends that the model makers train the model with efficient input variables. The function optimisation process attempts to intersperse data and the algorithm accurately, which might also involve collecting additional personal data to make the model more accurate. The more data is used for training the algorithm, the more likelihood of the model's accuracy, as it allows the model to learn the interrelationships between different variables. However, it also creates a Privacy-Accuracy trade-off because collecting more data can result in the loss of individuals' privacy.

Another trade-off we learnt in Part A was the 'Bias-Variance' trade-off. Though the choice of algorithm signifies the probable level of bias and variance, it is at the model training stage when the bias and variance errors can be plotted efficiently. In contrast, model training model makers try to achieve low bias and variance to yield good prediction outcomes. Unfortunately, achieving both low bias and variance is typically impossible. Non-linear algorithms with a high variance while completely representing the dataset on which they are trained (and thereby less biased) are at risk of overfitting with noise and are not generalisable.[444] Conversely, while showing generalisability across training datasets, linear algorithms with low variance are under-fitted as they do not capture representative datasets (making them highly biased).

The next challenge at the model training stage is assessing or evaluating the model for accuracy or precision. It is not limited to the challenge of the subjectivity of the makers to choose the metrics for evaluation, as stated in Part A. The challenge extends to the choice of the method, rather than only metric, due to technical reasons. One possible way of evaluating models is running the algorithm on the test dataset - the dataset split at the data partitioning stage - to predict the outcomes. However, it would defeat the purpose of test data, i.e. unseen data on which the model is never trained. Since the model training process happens repetitively, the test data would not remain 'unseen' after a few iterative cycles, making it prone to the same statistical harms as discussed above for the training datasets. Once the maker is satisfied finally - which is again subjective - after re-tuning and re-assessment, only then is the model used on test data to predict and provide the best estimations of how the algorithm will perform in the real world. At several stages, the accurate rate is predicted: first, while the model runs for the first time on training data, second after repeated iterative cycles of tuning trained data, and finally on test data. While

[444] Supra 392, pp. 700.

developing any regulation, policymakers and legal scholars must choose by specifying which estimate should be considered the most accurate and how it needs to be reported.

Another challenge discussed during the data collection and the model training stage was feature selection. As pointed out earlier, the ML pipeline is not linear, and stages intersperse within themselves; therefore, feature selection process can occur at both stages. Input variables that are a comprehensive and reductive representation of the output variable are chosen, which would mean an accurate outcome. While selecting features, there are choices to include a variety of variables that might result in the inclusion of those parameters which do not show an accurate account of statistical variation. As Professor Toon Calde and Indre Zliobaite have explained, '*It is often impossible to collect all the attributes of a subject or take all the environmental factors into account within a model*'.[445] It might be unintentional and sound to include or exclude a variable; such a choice can make the model non-generalisable. Professor Frederick Schauer defines such choices as '*simultaneously rational and unfair*'.[446]

While the abovesaid challenges that can result in unintentional discrimination are widely read, an emerging threat posed by big data remains unexplored, i.e., intentional discrimination, also called proxy discrimination. Whenever an AI discriminates based on a facially neutral characteristic, the risk of proxy discrimination depends upon the correlation between the output variable and the legally protected characteristic. Nevertheless, data mining techniques inevitably tend to find proxies of a variable. A process known as '*masking*' has the potential to cover for intentional discrimination that provides concealment of the fact that model makers have not considered an individual's protected characteristic.[447] Thus, data processing techniques not only provide means to commit illegal discrimination but also cover actual discrimination cases. Again, documentation and auditing, as discussed in detail in the last chapter, can provide a potential solution to the discrimination and privacy concerns highlighted.

[445] Calders, T., & Žliobaitė, I. (2013). Why unbiased computational processes can lead to discriminative decision procedures. In *Discrimination and privacy in the information society* (pp. 43-57). Springer, Berlin, Heidelberg.
[446] Shiner, R. (2005). Frederick Schauer, Profiles, Probabilities and Stereotypes. *Philosophy in Review*, *25*. Also read, Barocas and Selbst, Supra note 401.
[447] Ibid, Barocas and Selbst, pp. 692.

2.7. MODEL DEPLOYMENT

At the outset, the challenges in each of the three teams are discussed under the Model Deployment section in Part A. The *data scientists team* develops models on specific algorithms and particular data platforms. Such environments might be unfamiliar to the software engineers that make the seamless transition from model training to model deployment an error-prone process. It also raises the question of whether data scientists should build the model in a way suitable for implementation by software engineers. Another challenge for the team is making the model capable of running at scale. Models, especially those that provide predictions and classifications, thrive on a continuous data feed that makes the model prone to concept drifts or data drifts. It poses infrastructural constraints and needs to constantly re-upgrade and re-train the algorithm on new datasets. Such re-training, which might bring in new datasets, raises the challenge of '*reproducibility*' as adding new input variables might affect the outcome.[448] To maintain reproducibility, the same environment in which the model was made must be captured. In an educational setting, concept and data drifts can occur quickly, with new students entering the algorithmic gaze regularly. With each student depicting diverse qualities like learning engagement, facial emotions, peer relationships and others, educational ML algorithms will always require new data to predict accurate outcomes. With concept and data drifts changing over time with changes in habits, the data science teams in the education sector will have to investigate the intervals at which a model needs to be trained. Thus, visibility of the model performance becomes critical to determining its accuracy and whether it needs to be 'out of the market.

Second is the *DevOps team,* responsible for the backend infrastructure on which the model is deployed. The challenges at this stage are purely technical, and the chapter does not intend to deep dive into those; however, they are worth mentioning. Seamless transaction between data scientists and DevOps engineers is key to deploying models and is one of the most critical challenges for the latter team. Another challenge for them is ensuring the service's reliability and maintenance. It can be done by regularly monitoring and reproducing identical deployments as intended by data scientists. It would enable securing the ML model regarding authentication and access for data security purposes. Securing model access is as vital as securing access to a company's Intellectual property or clientele data.

[448] Henderson, P., Sinha, K., Angelard-Gontier, N., Ke, N. R., Fried, G., Lowe, R., & Pineau, J. (2018, December). Ethical challenges in data-driven dialogue systems. In *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 123-129).

The third is the *product team,* who is responsible for the impacts of the model, whether legally, ethically, morally, or economically. The first step by the team is to validate the model by bringing the prototype to the market and creating its value. But the challenge is whether to bring the model's prototype in a trial phase for specific customers and create a regulatory sandbox or simply roll out the model to the world, subjecting its benefits or flaws to everyone. The value of the model is also dependent on its prediction latency. Some use cases that require prediction in real-time, where slow running might severely harm the user. Another challenge for the product team is making the model accessible to all stakeholders. Once the model is deployed, it is not directly used by data scientists or software engineers. The teachers, students, principal, housekeeping staff or security guards will be in an educational setting. These stakeholders encounter the predictions and decide, entirely or partially, based on the prediction. The programmers or product developers are responsible for packaging the model in an accessible and legible user interface.

Part B attempts to prove that appropriateness and distribution are not framed or violated in isolation but are a product of context and thus right to privacy is 'cooked' within contextual relationships. Part B also pays attention to the bias and inaccuracy at each stage. The discussion of various stages proves that algorithmic technologies suffer from inaccuracies and invalid and biased outcomes that can creep in from any lifecycle stage. It is crucial to trace back such inaccuracies and biases to the initial stages as many harms and risks originate entirely during the designing stage of the model.[449] In such a scenario, regulation can be considered privacy preventive if it can ensure accuracy, validity and prevent bias.

CONCLUSION

The Indian government, rather than being technology deterministic, is 'information deterministic'.[450] It rightly observes information because of several 'data practices', noting that

[449] Supra note 392, pp. 668.

[450] Technological and Information Determinism might look identical, but the latter is a reduction of the former. While Technological Determinism, as various scholars argue, is a theory which assumes that technology is a driver of social, political, and economic change, Information determinism is not an established theory yet. Infact, academicians have also used the phrase like 'the *mythology* of '*information determinism*'. See Srinivasan, J., Finn, M., & Ames, M. G. (2015). Beyond Information Determinism to Information Orders: A New Framework for Policy. *iConference 2015 Proceedings*. However, the paper states that Information Determinism focuses on data collection and can motivate behaviours and influence policy actions. Such is the power of the data through which the thesis conceptualises the mythical theory of information determinism.

data in silos is invaluable but, once analytically processed, transforms into valuable information. *Data* is an engine transformed into 'information' by technologies like Artificial Intelligence, Machine Learning turning into Big Data. In most cases, such transformation is due to the internal functioning of the computing technology being unknown and invisible to the data subjects. Frank Pasquale refers to the said internal functioning as a 'black box' where the input data is processed by the computing system based on algorithms, invisible to the masses, and sometimes even the stakeholders who design the algorithms.[451] In addition to the opacity of processed data, input data is also embedded in normative and institutional contexts and the relationships of power and knowledge.[452] Thus, relying on information without understanding the input and the processed data, more specifically the churnings within the black box, can result in not comprehending the relationalities within which a breach of privacy gets cooked.

The influx of AI technologies, the surveillance they enable, inaccuracies and bias they emanate, creates a need for a data protection legislation that ensures an individual's privacy. To develop comprehensive legislation, one needs to understand the design of the technology i.e., how it uses data and how the right to privacy is compromised at each stage. Specifically, the current data protection legislations around the world lack the understanding of the machine learning (ML) lifecycle, i.e., how input data yields inferences, predictions or assumptions. To answer the question, the present chapter is divided into two sections. *Part A* explores the meaning of Artificial Intelligence and Machine Learning and dissects the black box operations. It contributes to understanding how a particular technology operationalises and treats data. *Part B* takes a closer look at the ML lifecycle and shows how the right to privacy is ignored, often diffused, and compromised at each stage. While Part A is slightly technical for the legal community, it should be borne in mind that it is written by a non-technical person, in a way helpful to future legislators and policymakers. Part B blends the technical jargon used in Part A to expose and enumerate the harms affecting individuals' privacy. By dividing the chapter, distilling the technical concepts, and tying them with the right to privacy, the chapter provides a comprehensive understanding of the complex and often unfamiliar territory for legal scholars and practitioners.

[451] Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.
[452] Chamuah A. and Bajpai H. (2022), Towards Responsible Data Practices for Machine Learning in India: Health & Agriculture. Digital Futures Lab, Goa.

By noting at all stages, the incessant and continuous flow of data, without the knowledge of the data subjects, variety of technical and economic choices made by the creators for their benefits, and different actors involved at each stage of the AI/ML lifecycle, the entire chapter depicts AI's close resemblance to being a modern age panopticon, surveillant assemblage and a surveillant capitalistic technology.[453] This chapter shows the said features of AI by peeking inside the black box and understanding the technicalities of each stage of the lifecycle, to derive a cohesive legislative plan. The present chapter highlights that whether it is the improper definition of the outcome variable, lack of diverse data, or choices of input data, all lead to discrimination and biased outcomes. Critics of data mining have emphasised wrong classifications or inaccurate predictions, but errors creep in at the problem identification stage itself. The available choices and the subjective knowledge to play with target variables and class labels are fodder for residing biases. The improper collection of data, overfitting of training datasets, using of wrong data also result in inaccurate or incomplete predictions. Algorithmic bias and wrongful predictions are not only discriminatory in nature but violate dignity and integrity of an individual, interfere with their decision-making capacities, and obscure the data that causes such bias and predictions, contributing to diminishing right to privacy. However, as the next chapter will show, the present data protection legislation in India excludes such discussions and is therefore ineffective in protecting right to privacy. The current data protection legislation overlooks the ways in which AI technologies or Aadhaar is currently operating, and the associated practices and its materiality. Thus, before suggesting recommendations the penultimate chapter discusses the inadequacies of the current legislation.

453

SIXTH CHAPTER

EXAMINING INDIAN DATA PROTECTION LEGISLATION

Technological change has always been seen as the progression factor of human civilisation. Therefore, the political belief in technology to resolve the messiness of governance does not sound astounding. The Indian Government's quest for technology, especially Artificial Intelligence (AI) applications, can be understood through previous chapters. Such reliance on AI by the government and private actors has also resulted in the large-scale aggregation of raw data, sorting it, and pooling it in a centralised repository. The intention behind the widespread collection of data and feeding into AI applications was spelt out in 2019 by India's chief economic advisor, Krishnamurthy Subramanian, that "*data should be treated as a public good*". Treating data as a public good signifies that it is open for the public and private actors to use datasets for generating knowledge and imparting social welfare. Supporting the fact that the state is ignoring its duties and transferring them to private actors, specifically in the education context, the CEA proposed that the information on students collected under various education schemes should be shared with private firms so that they can develop personalised tutoring products tailored to specific demands of the particular district. It is necessary to point out here, *firstly*, treatment of all education records as a public good is incorrect, and second, Section 8(1)(j) of the Right to Information Act[454] already classifies personal details of an individual as an exception to which no information can be sought. Thus, the latter statement sits at loggerheads with the first, by treating such information as a public good.

Which direction the data protection framework takes depends upon how data should be used, as a private or public good. Such framing has consequences on the right to privacy. Broadly, three approaches to the data protection framework can be seen. *First* is the lassiez-faire approach in the United States, where an overarching data protection framework is absent. The Right to privacy is codified, rather implicitly, in the First, Fourth and Fourteenth Amendments of the US constitution. Furthermore, several sector-specific legislations are tailored to protecting or securing individuals' data, like the Electronic Communications Privacy Act of 1986, Health Insurance

[454] (j) “information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information”.

Portability and Accountability Act, Right to Financial Privacy Act 1978, and Family and Educational Rights Protection Act. The laissez-faire approach, where private players handle and protect data while imposing stringent obligations on the state, is based on the USA's constitutional obligation to protect individuals' liberty free from state control. Such an approach treats data as a commodified good, in control of the individual in certain instances. Second is the EU approach of a comprehensive data protection legal framework in the form of GDPR, which is both sector and technology agnostic. GDPR and its predecessor, i.e., the Data Protection Directive, impose an equal obligation on government and non-government entities to protect individuals' data. Such obligation emanates from upholding the principle of individual dignity, wherein an individual determines how her data would be collected, used, and shared by public or private entities. The third approach, which is also the most recent, is the Chinese approach toward a Data protection framework. China has a series of interlocking legislation centred around data but primarily from an angle of national security. Whether we read the objectives of the Cybersecurity Law of China, 2017 or the recently enacted Data Security Law of China, 2021, the aims are to secure data protection, data localisation, protect cybersecurity, and govern the creation, use, storage and transfer of data; it is ostensibly in the interest of national security. Thus, the Chinese approach to the data protection framework emphasises the collective interest of individuals and the state rather than individual interest.

India is a reasonably recent addition among the countries aspiring to build a data protection framework and protect individuals' privacy. India's motivations for building a data protection framework might not be directly coincidental to one of the frameworks discussed above, but the present Bill borrows elements of each framework, examined in detail in the following subsection. The Bill encapsulates all three notions: liberty, dignity, and national security. However, the three notions should be read considering India's citizen-state relationship dynamics that take their inspiration from the Directive Principles of State Policy (DPSP) - Part IV of the Indian Constitution. DPSP is not directly enforceable on the state and is a guiding factor for citizens' progress. Article 39(b) and (c) of the Indian constitution direct the state to "*make policy towards securing distributed ownership and control of material resources and preventing the concentration of wealth to the common detriment*". If data can be interpreted as a material resource, the state must implement regulations for its creation, use, transfer, and storage in an equitable manner. Furthermore, due to the separation of powers doctrine, the Indian judiciary has the authority to impose an obligation on the state to put a data protection framework in place, as effectuated in the 2017 case of *K.S.*

Puttaswamy v. Union of India.[455] Thus, the Indian state is under a positive obligation to build a data protection framework while protecting citizens from the dangers of informational privacy emanating from public or private entities.

India has recently released its Data Protection Act that calls for provisions that can preserve privacy. However, as the chapter will show, it is bereft of any regulation around 'data practices' discussed in the last chapter. The chapter will also show that the existing provisions are also inadequate due to the changing technological advancements. Thus, the chapter will conclude by highlighting the inadequacies of the current legislation and thereby requiring a need for a legislative framework that resolves the concerns highlighted in previous chapters.

Before we delve into the intricacies of the different provisions of the Data Protection Bill, 2021, it is necessary to reproduce the legislative history of the Bill, specifically highlighting its changing objectives and purposes. In 2017, Supreme Court delivered a landmark judgement *KS Puttaswamy* v. *Union of India*[456], that explicitly recognised the Right to Privacy under the Indian constitution. One month before the judgement, the central government constituted a committee of experts to discuss data protection, led by Justice BN Srikrishna. A year into the committee's formation, it released the Srikrishna report discussing the contours of Data protection in the Indian context by relying on domestic and international jurisprudence.[457] Based on the Srikrishna Report, the government tabled the Bill before the Parliament in 2019. However, due to several concerns in the Bill, which are discussed below, the Bill was sent to the Joint Parliamentary Committee (JPC) for suggesting amendments. After almost two years, in December 2021, the JPC tabled a new version of the Bill called Data Protection Bill, 2021.[458] The Indian government finally released and passed the Data Protection Act before the Parliament in 2023. It is imperative to discuss the rejected and the current legislation, as they hold mirror to the ambitions and willingness of the Indian government in protecting individuals' data and informational privacy. Comparing the Srikrishna Report, PDP Bill, 2019, and the present Bill can help us understand the government's intentions behind providing or safeguarding individuals' Right to privacy via data protection. For

[455] *Puttaswamy*, Supra 267.
[456] Ibid.
[457] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, "*A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*", 2018.
[458] Report of the Joint Committee on The Personal Data Protection Bill, 2019, Seventeenth Lok Sabha, Lok Sabha Secretariat, New Delhi, December, 2021. Available at, http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf.

clarity and brevity reasons, it is helpful to divide the provisions of the present Bill into the following contours: a) Objectives, b) Consent and Notice Framework, c) Rights of Data subjects, and d) Obligations of Data Fiduciaries.

1.1. SCOPE & OBJECTIVE

The scope of the Bill can be ascertained by its change of the name from 'Personal' Data Protection Bill to Data Protection Bill. The removal of the word 'personal' broadens the scope of the present Bill, following the insertion of the definition of non-personal data. Clause 3(28) defines non-personal data rather vaguely as any '*data other than personal data*, essentially any data that is not personally identifiable of an individual. The Bill's scope, though diluted through Clause 92, gives the government unbridled power. Clause 92 is a non-obstante clause that states, "*Nothing in this act shall prevent the Central Government from framing any policy for the digital economy, including measures for its growth, security, integrity, prevention of misuse, and handling of non-personal data including anonymised personal data*". Clause 92 allows the government to frame any policy and provide any reasoning for such formulation without considering the present Bill. Such overriding power granted to the government entirely defeats the purpose of the Bill. Clause 3(28) follows the (JPC) recommendation number 1.15.8.4 includes personal and non-personal data, broadening the scope of the Bill; clause 92 dilutes it together.[459]

Srikrishna Report and PDP Bill 2019 emphasise building a collaborative digital economy that '*fosters sustainable growth of digital products and services and respects informational privacy*.[460] The justification for this lens in both documents lies in India's geography, i.e. Global South. The transformative potential of using Artificial Intelligence to deliver social welfare in sectors like health, education, agriculture, public benefits, and crime prevention is touted to be of immense benefit for developing countries like India. Both documents consider the objectives of protecting personal data and boosting the digital economy supplementary to each other and achieving the same constitutional objective of autonomy, liberty, and dignity. They construct the elements of informational privacy - autonomy, dignity, and liberty - as constitutive of a free and fair digital economy where an individual has power over their data, entities are responsibly sharing the data, and such sharing contributes to the nation's overall welfare. However, the report itself conflicts when it highlights AI's potential to cause discrimination, exclusion, and harm through the

[459] Supra note, 458.
[460] Ibid, pg. 8.

Cambridge Analytica episode.[461] It realises that the private actors and the state, for their respective purposes, have the potential to collect and process significant amounts of personal and sensitive personal data. Despite that, the report lays impetus in further paragraphs, stating that "*the growth of the digital economy…. must be equitable, rights-reinforcing and empowering for the citizenry as a whole*".[462] Thus, the report goes back and forth in balancing creating a digital economy and respecting informational privacy while simultaneously highlighting the dangers of AI.

Upon further examination of the report, it can be realised that the makers understand the conflict between the two balancing interests but are incentivised due to political and economic interests, as discussed in Chapter 4. The report explicates that rights should be evaluated in a given context of balancing the government's intention for the common good. It states, "*construction of a right itself is not because it translates into an individual good, …. but because such good creates a collective culture, where certain reasons for state action are unacceptable*".[463] It formulates two essential points: a) that a right comes into being when a collective interest is born and not merely an individual interest, and b) Right is not absolute, and thus the state can intervene, except in certain situations '*unacceptable*'. Thus, both documents establish the primacy of data protection and ensure the Right to privacy only to the extent of the nation's collective interest.

While keeping competing interests at loggerheads, the present Bill makes three minor yet essential amendments to the preamble that deserve attention. First is the inclusion of individuals '*digital*' privacy, making it clear that the data protection bill pertains explicitly to a specific facet of privacy, i.e., informational privacy. The second amendment is to the long list of the purposes of the Bill, namely, '*to ensure the interest and security of the state'*.[464] Ensuring the interest of the state can be said to be in alignment with the broader objective of the Bill of fostering the digital economy. The state's interests can be manifold, mysterious - as has not been defined in the Bill and change with the political leadership in power. Third, by way of the amendment protecting an

[461] Ibid, pg. 6.
[462] Id, pg. 9.
[463] Id.
[464] Among other purposes, a) provide protection of the digital privacy of individuals relating to their personal data, b) to specify the flow and usage of data, c) to create a relationship of trust between persons and entities processing the data, d) to protect the rights of individuals whose data are processed, e) to create a framework for organisational and technical measures in processing of data, f) to lay down norms for social media platforms (previously it was social media intermediaries), cross border transfer, accountability of entities processing data, remedies for unauthorised and harmful processing, g) to establish a data protection authority of India for the said purposes and for matters connected therewith or incidental thereto.

individual's data is an essential facet of informational privacy. Upon reading the three amendments together few things can be ascertained, that can form our basis for a comprehensive examination of the Bill; a) The Bill pertains to specifically protecting digital privacy, b) The Bill considers protecting individuals' data protection as a means of achieving informational privacy, c) Informational privacy is not an absolute right and can be interfered with to ensure the interest and security of the state. By keeping this understanding of the preamble of the Bill, we can now discuss other contours of the present Bill.

1.2. CONSENT AND NOTICE FRAMEWORK

Notice and consent frameworks are the bulwarks upon which the data processing of an individual is founded. Both frameworks can be viewed as an intuitive appeal to autonomy, dignity and liberty of an individual, necessary in a democratic society. Consent is enabled through providing a notice - a positive obligation on data fiduciaries to collect consent. There is a fair amount of literature that requires notice to be clear, specific, and informed. However, the meanings of such phrases need to be examined in a particular context. What clear or informed means for an adult would be very different to what a child would consider. Even within children, such concepts operate differently for different age groups.

Through the notice, the data fiduciary informs the subjects about the information they collect, how it is processed, to whom it is shared, and how the data is stored and kept securely. Providing notice has been seen as a means of "inner morality" or a distinction between arbitrariness and the rule of law.[465] Governments are obligated by the rule of law to act by the designed rules and regulations and make the citizens aware of how they will use their authority in given circumstances. It is necessary to provide sufficient information so that the citizens can make a choice and plan their personal affairs. Similar rules can also be seen in various consumer protection or product liability regulations whose main objective is to prevent buyers from seller coercion. In his seminal piece, Arthur Leff draws a parallel between the product liability and notice frameworks, stating that notice is akin to a product.[466] Leff states that similar to product liability regulations, if the data fiduciary fails to prepare a standard contract template, or should be subjected to a penalty. Since then, multiple domestic, international and sectoral legislations have

[465] Tucker, E. W. (1965). The morality of law, by Lon L. Fuller. *Indiana Law Journal*, *40*(2), 5.; Also read, Hayek, F. A. V. (2013). The road to serfdom. *Journal of Islamic Business and Management*, *219*(1239), 1-17.
[466] Leff, A. A. (1970). Contract as thing. *Am. UL Rev.*, *19*, 131.

included notice and consent mechanisms to enforce consumer privacy online. For instance, the Federal Trade Commission, which is guided by fair information practice principles (FIPPs), allows perusal of deceptive and unfair practices to protect the individual's autonomy, make citizens aware, and safeguard the integrity and security of the data - pillars of informational privacy.[467] The stated legislations and other regulations that mandate government, and other public & private players to disclose clear and specific information miss out on the context of the autonomy principle. It supposes that each individual can make better decisions upon getting the required information and, therefore, should be granted autonomy.[468] Similarly, in the case of children, it is presumed that they are not mature enough to be given the freedom to take decisions; instead, their guardians are in a better position. Everyone possesses a rational mind and should be free to take decisions is an approach also adopted by several courts, as we read in Chapter 2.

Ben-Shahar and Schneider provide three distinct reasons for the lawmakers to consider notice as an effective regime: cheap, easy, and effective.[469] They argue that notice regimes are easy to enforce, requiring more communication between contracting parties without large government expenditures. It also looks effective as more information; if it cannot help, it surely cannot hurt. If the question of information is presented to a data subject in terms of quantity, the majority will pitch in for more information. For such reasons, lawmakers rarely inquire into more profound questions of what a formal notice should look like, whether there is a need for sectoral notice templates, how should a data fiduciary provide mandated information which is legible, and whether children, especially those who are above thirteen want to make decisions, whether children or guardian want more information from data fiduciaries and what does informed consent entails. Thus, mandating disclosure - on which the entire notice and consent framework thrives - looks like a rescue in which data fiduciaries look visibly burdened, and data subjects are invisibly informed, continuing its incessant use and uncontrollable expansion.[470]

In the context of privacy, the failure of the notice and consent model is not limited to the legal dilemma of mandating disclosure. The model seems to have no answer to a set of practical

[467] Ly, B. (2017). Never Home Alone: Data Privacy Regulations for the Internet of Things. *U. Ill. JL Tech. & Pol'y*, 539.
[468] In late 1990s research started into the role of interfaces in impairing users ability to think around privacy and security, as well as their ability to make sound choices. Herzberg, A. (2009). Why Johnny can't surf (safely)? Attacks and defenses for web users. *computers & security*, *28*(1-2), 63-71.
[469] Ben-Shahar, O., & Schneider, C. E. (2017). The failure of mandated disclosure. *Russian Journal of Economics and Law*, (4 (44)), 146-169, pp. 136
[470] Id, pp. 138.

hurdles. The following hurdles are applicable to a set of fiduciaries who make their privacy policies directly available to the data subjects, like in the case of online websites. They cannot be made applicable to fiduciaries who carry out their services discreetly, for instance, the providers of CCTV cameras in Delhi schools, who do not even attempt to follow the mechanism. The fiduciary's identity was discreet until the attached Right to information request in the annexure was raised.

Nevertheless, seeking consent via providing information faces the first hurdle of unwillingness to read the notice. Not having the time to read notices is also understandable, especially after unique research by Carnegie Mellon researchers. McDonald and Cranor calculate that it would cost 781$ billion in worker productivity if everyone read the privacy policies they encounter online.[471] A student, irrespective of their age and maturity levels, hardly reads the terms and conditions of admission while signing up for the admission form. In some cases, the admission form is inaccessible to a child as the parents/guardian sign on behalf of the child without reading the privacy notices. A similar case is with online websites or school/classroom technology applications wherein either the notice is inaccessible or long enough for a child to understand. Unawareness or lack of interest in reading the admission form can be further motivated by long admission queues, parents' time constraints and trust in school authorities. In such a case, impliedly, the notice is expected to be read and explicitly affirmed by the parents/child's signature. Herein, the signature on the admission form is akin to a click-wrap contract on online websites, too which users are forced or impliedly considered to be aware of the terms and conditions. Sometimes, parents willingly consent to the school authorities or education providers and trade their children's privacy. However, in such cases, it should not be considered that the notice has been fully comprehended. In one dramatic example, in Delhi schools, most parents have readily agreed, in some cases requested, to access the live feed of the CCTV surveillance of their children's classrooms.

In addition to the time spent by consumers on a privacy policy, its legibility is another concern. The legibility of a person depends on varying capacities of individuals to process information, also referred to as cognitive limitations, their literacy, and inherent biases - what Herbert Simon labels

[471] McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *Isjlp*, *4*, 543. Also read, Bianca Bosker, Facebook Privacy Policy Explained: It's Longer Than The Constitution, Huffington Post (July 12, 2010), online at http://www.huffingtonpost.com/2010/05/12/facebookprivacy-policy-s_n_574389.html (Facebook's privacy policy contains more words - 5830 - than the U.S. Constitution.).

as '*bounded rationality*.[472] It is argued that privacy notices presume people have enough literacy, knowledge and expertise to comprehend notices and provide consent. Also, most privacy policies around the world are written in English, which is not everyone's first language, more so in India. Even where translations are available, it is unclear if translations do not lose out on words. Understanding an individual's capacity as limitless, one who can absorb information limitlessly is a misconception. Rather, the critics have pointed out that the harmful effects of information overload amount to '*consent fatigue*.[473] Excessive information can overwhelm the data subject, causing the tendency to skim through the notice, pick out information, and choose arbitrarily.[474] For instance, post-adoption of GDPR, 60% of websites displayed cookie consent notices to their users. The design and complexity of such notices are varied: some merely state that 'this website uses cookies, some provide a binary option of 'Agree' or 'Disagree', while others provide users to individually (de)select the types of cookies they want the website to store. While the first two designs provide too little choice, the latter design gives too much information for the user to read and agree upon. To prevent fatigue and secure users' time, the IAB released a Transparency and Consent Framework in 2019 that advocated for bundling consents. Using this framework, if the user provides consent to the browser, it passes the consent to the websites down the chain. The French court rightly criticised it, applying it against the GDPR framework. Consent should be continuous, sought for each purpose, and sought again once the purpose changes. Thus, a balance needs to be sought between providing enough detail to make people aware of data practices and not overwhelming them with too much information.

Information overload might put an individual in a position to rely on or 'latch on to earlier known information or emulate what others are doing - also known as '*anchoring*'.[475] For instance, a tech provider initiates CCTV surveillance in a school from one classroom as a trial. If a tech provider intends to nudge, it will provide the benefits of the surveillance in a particular classroom to the students, parents and school authorities, while hiding the details of the algorithm, type of data collected, with whom it is shared etc. Nudging can also happen by stating how students were

[472] Simon, H. A. (1997). *Models of bounded rationality: Empirically grounded economic reason* (Vol. 3). MIT press.
[473] Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019, November). (Un) informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security* (pp. 973-990).
[474] Dalley, P. J. (2006). The use and misuse of disclosure as a regulatory system. *Fla. St. UL Rev.*, *34*, 1089.
[475] Ripken, S. K. (2006). The dangers and drawbacks of the disclosure antidote: toward a more substantive approach to securities regulation. *Baylor L. Rev.*, *58*, 139.

willing to share their information because they can understand their learning engagement comprehensively. It can anchor other students and their parents to consent to CCTV deployment to get tangible results. In addition to anchoring, students can also provide consent by following the advice of their teachers or acting out of the influence of someone like their role models, which Ripken calls '*influence of self-esteem.*[476] Thus, decisions made because of anchoring or under the influence of someone involve invasive disclosures, which might bring immediate gratification or some access to desired services but are subject to privacy costs in the long term.[477]

Humans often make decisions based on their cognitive abilities, biases and imperfect heuristics. If one has the means to transgress an individual's psychological dimensions, it can affect their actions and choices. Thaler and Sunstein call such effects '*nudging*'.[478] Given the effect nudging can have on children's encounters with technology and their autonomy, the relationship between nudging and consent warrants attention. Nudging attacks, the 'free' element of consent and acts as means of coercion. It is fair to assume herein that when nudging vitiates consent, it renders consent impermissible. Amidst numerous proposals, some scholars advocate for certain factors that allow permissible nudging;[479] others are sceptical and claim that nudging constantly subverts decision-making.[480] According to Kiener, the debate has moved towards three sets of conditions when nudging is permissible, against which children's consent should be evaluated: *Easy Resistibility*, *Transparency* and *Rationality*.[481] The first condition where nudges can be permitted is if they can be easily resisted. If the person does not feel any psychological coercion and does not have to apply any specialised skills to resist nudging, it can account for easy resistibility. The second condition is transparency, which has also been emphasised in manipulation cases. The availability of information regarding the existence of nudging, how nudging is practiced, and the intention behind nudging amount to its transparency. The final condition for permissible nudging exists if nudging appeals to someone's irrationality, exploit it or out-manoeuvres it. It amounts to

[476] Loewenstein, G. (1996). Out of control: Visceral influences on behavior. *Organizational behavior and human decision processes*, *65*(3), 272-292.
[477] Acquisti, A. (2004, May). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on electronic commerce* (pp. 21-29).
[478] Kiener, M. (2021). When do nudges undermine voluntary consent? *Philosophical Studies*, *178*(12), 4201-4226. Also, Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., ... & Wilson, S. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, *50*(3), 1-41. Thaler and Sunstein, define nudging in the form of an acronym NUDGES: iNcentives, understand mappings, Defaults, Give feedback, Expect errors, Saliency.
[479] Saghai, Y. (2013). Salvaging the concept of nudge. *Journal of medical ethics*, *39*(8), 487-493.
[480] Wilkinson, T. M. (2013). Nudging and manipulation. *Political Studies*, *61*(2), 341-355.
[481] Kiener Supra note 478.

nudging when it does not consider that humans are rational and are capable of making choices, also referred to as '*process rationality*'.[482] In such cases, it leads to information asymmetry i.e. a situation where one agent collecting data has more information than the agent providing the data upon a nudge.[483] The lack of equal information between agents can lead to structural consolidation of power, as scholars have noted in the context of Big Tech companies. In the education context, Information asymmetry can be seen in multiple layers of relationships. It is not necessary that nudging is done only by one actor; rather, it can have a downstream impact. For effective technology deployment, tech providers rely on school authorities, who ask the teachers to collect student data. As we saw in Part A, teachers are the primary data collectors, but by way of delegation, they sometimes ask the students to gather, sort or aggregate data of the entire class. Thus, asymmetry is prevalent between teachers and students, students and students, school authorities and students, tech providers and school authorities. Often teachers and students are also unaware of the purpose behind their data collection practices, let alone the subjects whose data is being collected.

The applicability of permissible nudging in cases of Artificial Intelligence applications runs into grey territories, questioning whether nudging can ever be permitted in the context of informational privacy. For instance, it is challenging to resist Google's artificial intelligence when it automatically suggests searches, and the user is encouraged to cling to the algorithm's choices. Similarly, technology companies play on parents' anxieties about their children's safety and security and their guilt about missing key childhood moments.[484] By not disclosing the intention behind marketing the use of surveillance devices, tech companies and sometimes school authorities engage in a soft or libertarian paternalistic approach of nudging.[485] In such an approach, the user has not forbidden any options but is nudged to behave in a certain predictable way.[486] Increasingly, parents are providing consent as they are allowed to continuously monitor their

[482] Schmidt, A. T. (2019). Getting real on rationality—Behavioral science, nudging, and public policy. *Ethics*, *129*(4), 511-543.
[483] Acquisiti, supra note 477.
[484]Hofer, B. K., Souder, C., Kennedy, E. K., Fullman, N., & Hurd, K. (2009). The electronic tether: Communication and parental monitoring during the college years.
[485] Nudging - a soft paternalistic approach - lies somewhere between strictly paternalistic and strictly libertarian approaches. Strictly paternalistic approach impose decisions by way of regulation like on cigarette smoking. Whereas strictly libertarian advocates for self-regulation approaches that provides the user with a variety of options. For more details read, Privacy and human behaviour in the age of information.
[486] A. Acquisti. Nudging privacy: The behavioral economics of personal information. IEEE Security and Privacy, 7(6):82–85, 2009.

child's whereabouts with no need to discuss such details on phone. The prevailing nudge herein is the notion of 'parental responsibility that steers the parents to provide consent. However, due to a lack of transparency, the parents are procedurally making irrational decisions. Providing consent by trusting in manipulative marketing causes biased decision-making, vitiating consent. Thus, the three conditions of permissible nudging do not squarely apply in cases of seeking students or their parent's consent. There are hidden factors which influence the decision of one to provide or forego consent, concluding that consent at best is broken and, at worst, is biased. In his paper on nudging and voluntariness of consent, Kiener arrives at the same conclusion though evaluated from the medical consent context. He concludes by stating three nudging practices which vitiate consent, i.e., a) if it controls the decision by overlooking the balanced evidence, b) if makes the person less rational or exploits the already existing irrationality, and c) if it forces an individual's procedural rationality into serving other's needs at the expense of its own.[487]

The discussion above shows that simply having a consent policy in the legislation is not enough. There needs to be an effective framework in which a child has enough control and power on the decisions made for them. The next section will provide recommendations as to how to optimise consent in the AI age, highlight the limits of parental consent and suggest ways to involve child while designing, developing, and deploying a technology to safeguard their privacy.

1.3. **USER RIGHTS**

AI technologies rely on unpredictable data and values to produce inferences and predictions, paving the way for biased, discriminatory, and privacy-invasive decision-making.[488] Such technologies use inferential analytical methods to make inferences or predictions about individuals shaping our perceptions of them. The said technologies impact our intuitive minds, shaping our power and control over information (a crucial constituent of informational privacy, as shown in Chapter 3). Due to the continuous erosion of our informational privacy - and thereby autonomy - it is imperative to discuss the meaning of the rights provided to data subjects in the current legislation. It is necessary to situate and contrast the rights with the novel risks that inferential analytics poses while designing, developing, and deploying AI technologies.

[487] Kiener, supra note 478.

[488] For technical understanding refer to Supra note Part B. See more, Brent Daniel Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter & Luciano Floridi, The Ethics of Algorithms: Mapping the Debate, *Big Data & Society*, July–Dec. 2016, at 1–2.

The previous drafts of the Indian data protection bill have provided certain data subjects rights, including a) the Right to confirmation and access wherein the data subject has the Right to obtain in writing a summary of processing activities being conducted by the data fiduciary, b) Right to correction and erasure, allows the data subject to correct, complete, update, or erase its data, c) Right to data portability, where the data subject can have their data transferred to any other data fiduciary and d) Right to be forgotten, which allows the data principal to restrict or prevent the continuing disclosure of personal data. One of the other rights embedded under the Right to data portability is the Right to receive data in a structured format, including the data which has been generated during the provision of services and data which forms part of any profile on the data principal, where the processing has been carried out through automated means. Though it is unclear why such Right has been embedded under a different Right, such inclusion by the legislators should be lauded. Including the data generated while providing services or profiling the data subject implies inferences, predictions, and assumptions (collectively referred to as 'inferences' below) generation about an individual by an AI technology at any stage of processing. The Right to inferences forms the bedrock for all the rights mentioned above. It is because disclosure of inferences addresses why specific data was chosen/accepted to draw a particular inference, what processing methods were used to yield inferences, and whether the data and processing methods are accurate and reliable. Through inferences, the machine lifecycle can be backtracked to understand its inner functioning, contributing to greater transparency and accountability of the 'black box'. Thus, it is necessary to examine the said Right significantly when it supplements and strengthens other mentioned rights.

1.3.1. **A RIGHT TO INFERENCES**

Even if we assume that the Indian legislators intended to include the Right to Inferences under Right to Data Portability, globally, the jurisprudence on inferences is unclear. For instance, the European Court of Justice (ECJ) has made it clear that data protection law is not meant to ensure the accuracy or decision-making of the technology or to make the processing transparent. In short, the ECJ remarks that data fiduciary's rights are protected at the collection and processing stage but not at the evaluation stage.[489] The ECJ also clarifies that if the data fiduciaries intend to

[489] See Case C–28/08 P, *European Comm'n v. Bavarian Lager Co.*, 2010 E.C.R. I–6055, pp., 49–50; Case C–434/16, *Peter Nowak v. Data Prot. Comm'r,* 2017 E.C.R. I-994, pp., 54–55; Joined Cases C–141 & 372/12, YS, *M and S v. Minister voor Immigratie, Integratie en Asiel*, 2014 E.C.R. I-2081, pp., 45–47.

challenge the evaluation, recourse must be sought through sectoral data protection laws.[490] It is what the Article 29 working party also recognises that "*more often than not, it is not the information collected in itself that is sensitive, but rather, the inferences drawn from it*".[491] The scholars like Tene and Polonetsky also similarly argue that it is not the accuracy of the raw data which is to be scrutinised but the accuracy of the inferences drawn from the data.[492] However, as shown in Part A and Part B of this chapter, biases enter the system at the data collection or problem identification stage itself. It is the result of human choices and opinions at the first stage of the ML lifecycle, which gives birth to inferences or, as some refer to, ' *inferential analytics*.[493] Thus, it is equally essential to scrutinise data collection practices (not only from a consent or notice point of view) and predicted inferences.

Inferences, assumptions, and predictions are harmful to individuals by their inherent unpredictable nature. The digital profile that gets persistently built on inferences creates an individual's identity, violating an individual's self-made personality. In fact, the ECHR has a long-standing jurisprudence in linking the Right to personality to the Right to privacy. In *Deklerck v. Belgium*, the court stated that guaranteeing the development and fulfilment of personality is the primary goal of Article 8 of the ECHR.[494] Further, in *Grabenwarter v. Pabel*, the court enunciated that "*lifestyle, life choices, and way of life have to be protected from state intervention. Independent life choices require the free and unobserved development of own abilities.*" Such spaces are meant to be protected to allow individuals to function freely and exercise their autonomy. In the face of uncertainty in developing one's own personality, it can lead individuals to self-censorship and alter their behaviours - referred to as the "*autonomy trap*".[495]

---

[490]Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Colum. Bus. L. Rev.*, 494.

[491] Article 29 Data Prot. Working Party, Opinion 03/2013 on Purpose Limitation, at 47, 00569/13/EN, WP203 (Apr. 2, 2013), https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2013/wp203_en.pdf [https://perma.cc/X6PC-825X].

[492] Tene, O., & Polonetsky, J. (2012). Big data for all: Privacy and user control in the age of analytics. *Nw. J. Tech. & Intell. Prop.*, *11*, xxvii.

[493] Privacy International (Nov. 8, 2018), http://privacyinternational.org/advocacy-briefing/2426/our-complaints-against-acxiom-criteo-equifaxexperian-oracle-quantcast-tapad (on file with the Columbia Business Law Review);

[494] *Deklerck v. Belgium*, Application Number 8307/78. Similarly, in *Peck v. United Kingdom*, (2003) 36 EHRR 41. The court talks about right to personality and right to personal development. Also, *Grabenwarter v. Pabel*, EMRK5 § 22 Rz 1ff.

[495] Zarsky, T. Z. (2002). Mind your own business: making the case for the implications of the data mining of personal information in the forum of public opinion. *Yale JL & Tech.*, *5*, 1.

Due to the persistent use of AI technologies over time, space and systems solidify an individual's identity, undermining their Right to experiment or start their life again. In such a context, the present data protection legislation is yet to come to terms with effectively informing the data fiduciary about the data and its inferences. The Indian legislation obligates the fiduciary to provide the generated data to the subject in a structured format in the case of automated decision-making. It is open to our interpretation of what is meant by structured format and if providing generated data in a format proves an effective right. It is also unclear whether it includes how the generated data is produced, the criteria and methods used to process the data, or the choices taken by the data scientists. Herein, the Right to provide generated data conflates intersects with the Right to confirmation and access, under which the fiduciary is obligated to provide processing methods. However, like the Right to inferences, the effectiveness of this Right also remains. A right is ineffective if it cannot be meaningfully exercised. If the data subject cannot understand the processing methods and their implications, it is futile to provide the information. Thus, whether it is the Right to confirmation or the Right to inferences, the legislation's effectiveness and enforceability could have been much clearer if supported by another right - '*Right to Explainability*'.[496] It is referred to as the ability of the machine learning to give reasons for estimations. The next chapter will illustrate the importance of providing reasons behind lifecycle choices enabling data subject's trust in the technology and strengthening user's rights.

1.4. **DATA FIDUCIARIES**

Data Fiduciaries, akin to data controllers in the GDPR, collect data from the data principal and are responsible for its fair processing, sharing and storage. Srikrishna Report used the term '*fiduciary*' for the first time, keeping in mind the intention of the data principal to keep their data secure. The Fiduciary relationship has long been recognised in the context of agency law - patient - doctor, lawyer-client, husband - wife, and trustee - beneficiary. Trust and duty of care are the two cornerstones of fiduciary relationships.[497] Given the information asymmetry and lack of trust in the digital realm, the conceptualisation of data controllers as fiduciaries looks intuitively attractive. However, the concept has faced widespread criticism as it overlooks the existing business models that thrive on ubiquitous data collection.[498] Despite criticism, the use of the word 'fiduciary' has found constant mentioning, be it the 2019 or the 2021 Bill. Thus, it is necessary to

[496] For details, refer to Chapter 7.
[497] Kapoor, A., & Whitt, R. S. (2021). Nudging towards data equity: The role of stewardship and fiduciaries in the digital economy. *Available at SSRN 3791845*.
[498] Khan, L. M., & Pozen, D. E. (2019). A skeptical view of information fiduciaries. *Harvard Law Review*, *133*(2), 497-541.

understand the benefits and dangers of using the term 'fiduciary' and whether all data processing relationships in a school context are fiduciary. It should also be borne in mind that while the USA also conceptualises the concept of 'information fiduciaries in the informational privacy context, the GDPR does not find any mention.[499]

Miller regards those relationships as '*fiduciary*', in which one of the transacting parties is vulnerable to another reposes trust and faith in the other.[500] According to Frankel, the main characteristic of a fiduciary relationship is when the fiduciary substitutes the beneficiary to meet a specific goal.[501] In this, the beneficiary gives agency to the fiduciary to meet a goal. However, this creates a potential for abuse by the agent - acting out of self-interest. Also, recognising fiduciary relationships advocates favour paternalistic approaches thereby limiting the autonomy of the beneficiary. In order to enhance autonomy and minimise abuse, the law steps in to create a more level playing field, casting obligations on the fiduciary. Frankel also notes that the fiduciary relationship is different from any other law, such as contract law, in which good faith is not explicitly recognised. While parties in a contract can act in self-interest, in a fiduciary relationship, the fiduciary is obliged to keep its interest subservient to the beneficiaries. In the case of the *Central Board of Secondary Education and Anr. v. Aditya Bandopadhyay and Ors.*, the Supreme Court has defined the word fiduciary as:

> "*A person having the duty to act for the benefit of another, showing good faith and candour, where such other person reposes trust and special confidence in the person owing or discharging the duty*"[502].

The Indian courts have taken positions based on each contextual relationship and recognised its fiduciary and non-fiduciary aspects. In the case of *Raju Sebastian and Ors.* v. *Union of India,*[503]

[499] Ibid.
[500] Miller, P. B. (2013). Justifying fiduciary duties. *McGill Law Journal*, *58*(4), 969-1023.
[501] Frankel, T. (1983). Fiduciary law. *Calif. L. Rev.*, *71*, 795.
[502] *Central Board of Secondary Education and Anr.* v. *Aditya Bandopadhyay and Ors.*, 2011 8 SCC 497. For further elucidation of court's defining of such relationships, can refer to *Treesa Irish w/o Milton Lopez v. Central Information Commission and Ors. 2010*, wherein the court stated the following conditions for a relationship to be considered as fiduciary: "a) The fiduciary has the scope for the exercise of some discretion or power, b) The fiduciary can unilaterally exercise that power or discretion so as to affect the beneficiary's legal or practical interests, c) The beneficiary is peculiarly vulnerable to or at the mercy of the fiduciary holding the discretion or power, d) The fiduciary is obliged to protect the interests of the other party".
[503] *Raju Sebastian and Ors.* v. *Union of India and Ors.*, 2017 10 SCC 1.

the court opined in context of personal data where banks were held to be in a fiduciary duty to their customers. The banks are obliged to protect the secrecy of an individual's information, and no third party can request the information available with the bank unless disclosure is mandated by law. Specifically, courts worldwide have concluded based on each situation and the underlying interrelationships. in the schools' context. For instance, the US courts have opined that school personnel do not owe a fiduciary obligation to students when they are engaged in a legitimate purpose for which they are employed, i.e., administering grades and imparting knowledge. Conversely, school personnel owe a fiduciary obligation if they engage in illegitimate conduct like sexual harassment or abuse - which is wholly outside the role they are recruited for.[504] Similarly, if the school administration is holding money or administering funds for students, they owe a fiduciary obligation. The US courts addresses such fiduciary obligations under the '*loco parentis'* doctrine, meaning 'in the place of a parent'.[505] For instance, in *McMahon* v. *Randolph-Macon Academy*, the staff member developed a sexual relationship with the student.[506] The court, while imposing a fiduciary duty on the staff member, stated that such imposition restricts fiduciary actions to those in the interest of the beneficiary. Especially in a boarding school, where minors are kept in custody, the school personally are fiduciaries under loco parentis doctrine, as the school authorities must take in the interest of the student. It shows that the courts use the doctrine to establish a fiduciary duty of school authorities to children. However, there are a plethora of non-loco parentis cases that recognise a fiduciary duty. In *Doe* v. *Terwilliger,* the student brought a claim against the school athlete coach due to several instances of intentional touching.[507] The court stated that if there is any fraud, misconduct or misappropriation on behalf of the fiduciary, misusing superiority - of his knowledge, skill, expertise, or position -breaches its fiduciary duty. The court also noted that fiduciary duty should not be confined to a particular doctrine but evaluated case-to-case basis. The commentators have also supported this point, as there are several factors in an educational context that determine whether the relationship is fiduciary or not. As Scharffs & Welch note, in assessing the magnitude of fiduciary duty and its breach,

[504] Also, in another case of *In Re the Arbitration between Howell Public schools and Howell Education Association*, *1991 WL 692932 (Arb.) (1991) (Brown, Arb.)*, the teacher took commission from the travel agent while booking a trip to Washington D.C. for her students. She herself testified in the court that while planning for the trip she acted both as the teacher and in place of students' parents. The court accepted and stated that "The teacher's role is of loco parentis in which the teacher is bound to take reasonable care of the students in their custody. This responsibility creates a fiduciary duty."

[505] *DeJohn* v. *Temple University*., 537 F.3rd circuit, 2008, opined that public elementary and high school administrators have a unique responsibility to act in loco parentis, unlike their counterparts in public universities.

[506] No. 97-11, 1997 WL 33616521 (Va. Cir. Ct. June 16, 1997).

[507] *Doe v. Terwilliger*, 2010 Ct. Sup. 13190, 49 CLR 1 (Conn. Super. Ct. 2010).

specific parameters can be taken into consideration: actual power entrusted to the fiduciary, experience of the fiduciary, status of the beneficiary, history and duration of their relationship, degree and cause of trust in their relationship, among others.[508]

It should be kept in mind that there are several case laws and commentaries rejecting the proposition that college educational authorities are in loco parentis relationship with students.[509] It is primarily because of students' vulnerability and rationality in a school versus in a higher institution. Students in a school constitute a vulnerable population, prone to harm and exploitation from teachers, school authorities and education technology providers, who have the power to do so. Whether through the application of the loco parentis doctrine or not, it becomes clear that courts acknowledge the fiduciary relationship between schools and higher authorities. Henceforth, it makes sense why courts create differentiation between college and school students in the context of the teacher-student fiduciary relationship, that is primarily based on their age.

The courts in India seem to have adopted similar analogies to those of US courts in determining fiduciary relationships in the educational context. In the case of *Bihar School Examination Board v. Suresh Prasad Sinha*[510], the Supreme Court held that the examination authority does not owe a fiduciary duty to students. Though the case law not directly attributable to our thesis, the reasoning is worth mentioning. The court opined:

> *"When the Examination Board conducts an examination in discharge of its statutory function, it does not offer its "services" to any candidate. Nor does a student who participates in the examination conducted by the Board, hires or avails of any service from the Board for a consideration….. The process is not therefore availment of a service by a student, but participation in a general examination conducted by the Board to ascertain whether he is eligible and fit to be considered as having successfully completed the secondary education course."*

[508] Scharffs, B. G., & Welch, J. W. (2005). An analytic framework for understanding and evaluating the fiduciary duties of educators. *BYU Educ. & LJ*, 159.
[509] William A. Kaplin, The Law of Higher Education 5-7 (2d ed. 1985). *Buttny* v. *Smiley*, 281 F. Supp. 280, 286 (D. Colo. 1968) (noting "that the doctrine of '*In Loco Parentis*' is no longer tenable in a university community");
[510] (2009) 8 SCC 483.

To evaluate the fiduciary relationship, the Supreme Court brought in an element of 'service' and 'consumer' that it finds absent between the examination board and the student, hence no fiduciary obligation. In another case of *Avinash Nagra* v. *Navodaya Vidyalaya Samiti and Ors.*, the Supreme Court concurring with the US Supreme Court judgements discusses the loco parentis doctrine.[511] It involved the circumstances of misconduct by a school authority with a student who was unbecoming of a teacher. The court answered negatively on whether the conduct of the school authority was befitting in the context of entrusted responsibilities of trust and care. Even without enough Indian legal jurisprudence on the doctrine, it is fair to assume that, on the question of fiduciary relationships in the education context, Indian courts are treading the path of the US court judgements.

1.4.1. INFORMATION FIDUCIARIES' ENIGMA

In an informational privacy context, the Srikrishna Committee Report has termed entities responsible for collecting, using, and sharing data as '*data fiduciaries*'. As explicitly expressed in the said report, the phrase has been taken from the view expressed by Jack Balkin's concept of Information Fiduciaries conceptualised over a series of papers.[512] By referring to Balkin's concept, the report misses two essential pointers: first, that it was Kenneth Laudon who coined the phrase in the early 1990s, from a markets perspective, and second, that Balkin discusses the phrase while showing a conflict between First Amendment rights of the US Constitution (freedom of speech and expression) and data protection law, explicitly targeting advertising-based business models. Laudon and Balkin's analysis of information fiduciaries also contradicts the definition according to a data fiduciary in the Indian PDP Bill. Balkin regard digital companies as information fiduciaries who accumulate, analyse, and sell their data for profit. On the contrary, the Bill encompasses "*any person, including a state, a company, juristic entity, or any individual alone or with others determining the purpose and means of the processing of personal data*" as a data fiduciary. Digital companies cannot be equated with a state because of their differing roles, goals, functions, and responsibilities towards the data principal. Also, Balkin accepts that the fiduciary obligations of trust, care and confidentiality cannot be imposed on digital companies (specifically the ones she mentions like Facebook, Twitter, and Uber) in the strictest and traditional sense, instead in a limited manner.[513] Due to the committee's silence, the lurking question is about the

[511] (1997) 2 SCC 534.
[512] The paper referred by the Srikrishna Committee is Jack M Balkin Information Fiduciaries and the First Amendment. However, the idea was first promoted in a 2014 blog post, Laudon, K. C. (1996). Markets and privacy. *Communications of the ACM*, *39*(9), 92-104.
[513] Balkin, J. (2018). Fixing Social Media's Grand Bargain. Aegis Series Paper No. 1814.

intention behind adopting the phrase and if the Bill suggests equating digital companies to a state.[514]

While the intention of the phrase's adoption remains unclear, it is necessary to unpack Lina Khan and David Pozen's sceptical look at Balkins' information fiduciaries[515] and its relevance in the Indian context. Balkin explains the concept by using Facebook as an example of a digital information fiduciary, focusing on its services, business models, and market dominance structure. He emphasises and compares Facebook with traditional fiduciary relationships where individuals pass on the information to professional experts to obtain valuable and expert services.[516] Like Facebook, an individual submits information to the organisation in return for their service to connect with the social community. It is also important to note herein that whether in the case of Facebook or traditional relationships, the client cannot understand the complexity of provisioning such services. Because of such expertise and complexities, the data principal expects trust, care and confidentiality goals, thus casting obligations on the data fiduciary. Balkin argues that an information fiduciary can pursue such goals without disrupting the business model of providing services in exchange for data monetisation.[517]

Khan and Posen begin their critique by assessing Balkin's argument against the legal status quo of organisations.[518] In the Indian context, we can begin the examination of corporations from the Companies Act 2013 and its underlying fiduciary obligations. Before the Companies Amendment Bill, 2013, the directors of a company owed a fiduciary duty only to the company's shareholders. Though the term fiduciary is absent from the original companies Act, 1956 or the amendment Bill, the Indian courts have referred to the director's obligations as fiduciary towards the shareholders. The Supreme Court in *Dale and Carrington Investors Private Limited and Ors.* v. *P.K. Prathapan and Ors.*, court states:

[514] Section 26 of the PDP Bill classifies certain data fiduciaries as significant data fiduciaries, depending upon volume of personal data processed, sensitivity of personal data processed, turnover of the business and risk of harm posed by the processing. It is believed to target certain types of social media platforms. Still, the question remains whether the businesses which not significant data fiduciaries are at the same platform as other data fiduciaries like state.
[515] Khan, L. M., & Pozen, D. E. (2019). A skeptical view of information fiduciaries. *Harv. L. Rev.*, *133*, 497.
[516] Balkin, J. M. (2017). Free speech in the algorithmic society: Big data, private governance, and new school speech regulation. *UCDL Rev.*, *51*, 1149. Balkin further states that though the client submits information to the fiduciary to get in return the latter's expertise, however, the client is unable to comprehend the information given by the latter.
[517] Balkin, J. M. (2015). Information fiduciaries and the first amendment. *UCDL Rev.*, *49*, 1183.
[518] Supra note 515, pg. 501.

> "*Fiduciary capacity of directors enjoins upon them a duty to act on behalf of a company with utmost good faith, utmost care and skill and due diligence and in the interest of the company they represent. They have a duty to make full and honest disclosure to the shareholders regarding all important matters relating to the company*".[519]

Post-2013 amendment Bill, the Indian law under section 166 of the companies act, has taken a more pluralistic approach. It encompasses directors' obligations towards not only the shareholders but also the interests of 'non-shareholder constituencies' (referred to as the stakeholders). Since Indian independence, the primacy was vested in the shareholder's interest; however, in certain instances of 'public interest, wherein the companies' affairs are carried out in a manner prejudicial to the public interest, non-shareholders affected parties could ask for redress.[520] The 2013 Act embeds the notion of public interest along with the shareholder's interest within one clause in an attempt to treat both at an equal footing. Section 166(2) of the 2013 Act reads:

> *"A director of a company shall act in good faith in order to promote the objects of the company for the benefit of its members as a whole, and in the best interests of the company, its employees, the shareholders, the community and for the protection of the environment."*

Section 166(2) mentions two positive obligations: one to promote the objects of the company and the other to act in the best interests of the company, indicating that the clause seems to be distinctive in two parts. It is the latter where the director of a company is obliged to act in good faith towards shareholders and other 'stakeholders'. The provision does not explicitly recognise the specific stakeholders and leaves the meaning of community vague. However, when inserting the said section, the Ministry of Corporate Affairs relied on the Parliamentary Standing Committee on Finance that directors' duty should be beyond the shareholders due to their obligations under Corporate Social Responsibility (CSR).[521]

---

[519] (2005) 1 SCC 212.

[520] Refer to Section 394 and Section 397 of Indian Companies Act, 1956.

[521] Twenty-first Report, Standing Committee on Finance (2009-2010) (Fifteenth Lok Sabha), The Companies Bill, 2009 (Ministry of Corporate Affairs), Lok Sabha Secretariat, New Delhi, August 31, 2010. Available at:http://www.prsindia.org/uploads/media/Companies%20Bill%202009.pdf. It is important to note herein that the Standing committee recommended to the ministry based on Institute of Company Secretaries of India (ICSI) specific reference to CSR.

The relevance of these provisions become much clearer upon discussing the UK's Section 172 of the Companies Act, 2006 which also talks about director's fiduciary duties. Section 172 reads as follows:

> *(1)A director of a company must act in a way that he considers, in good faith, would be most likely to promote the success of the company for the benefit of its members as a whole, and in doing so have regard (amongst other matters) to —*
>
> *—----------*
>
> *(d) the impact of the company's operations on the community and the environment,*
>
> *—----------*

The UK act asserts that the directors should act in good faith, primarily to promote the company's success for the shareholders' benefit. It also states that directors should regard the community and the environment while benefiting the shareholders. As one author notes, the traditional conception of stakeholder interests is given primacy, with companies' operations' effect on the environment, community and others being seen as a means of generating shareholder profit due to the usage of the phrase: '*have regard to*.[522] Authors have termed such a model the Enlightened Shareholder Value Model (ESV). So, Indian law does not have the '*have to regard*' approach whereby shareholders are placed on a higher pedestal than stakeholders. While India follows a more pluralist approach, giving greater protection to stakeholders, the UK adopts the ESV model.

Turning back to the question of corporations owing fiduciary obligations can also be placed in the education sector. As shown in Chapter 3, burgeoning organisations provide various technologies through services to Indian schools. In return, schools are getting bulk information about students, often handled by corporations (referred to as third-party providers in Chapter 4), giving both school authorities and corporations increasing capacities for surveillance and control. Focusing on education products and services corporations herein, the law places fiduciaries with opposing loyalties contradicting each other.[523] If we read the UK approach, the director of a company has to primarily prioritise the benefit of the company and its shareholder, driving it to maximise the economic value of the company. If we dissect the Indian approach, though the shareholders and

[522]Naniwadekar, M., & Varottil, U. (2016). The stakeholder approach towards directors' duties under Indian Company Law: a comparative analysis. *Mahendra Pal Singh, The Indian Yearbook of Comparative Law*, 95-120.

[523] Miller, P. B. (2014). Multiple loyalties and the conflicted fiduciary. *Queen's LJ*, *40*, 301.

the public interest are given the same pedestal, the law asks to primarily promote the company's objects while balancing the public's best interests. One such corporation, also mentioned in Chapter 4, is Entropik Tech which provides emotional AI products to Indian schools and colleges. According to Section 166 of the Companies Act, 2013, Entropic Tech's director owes a fiduciary duty to the 'community'. In light of the absence of jurisprudence on the meaning of the word 'community' in India, we can take inspiration from UK Court's jurisprudence. In the UK, the word community encompasses the public, end-users, and other stakeholders. In Entropic Tech's case, the community would include stakeholders like school authorities, students, teachers, suppliers etc., towards which it owes a fiduciary obligation.

Entropic Tech's objective is to redefine offerings and experiences by reading human emotions accurately and meaningfully.[524] It is not hard to imagine how the interests of such corporate stakeholders and the public can diverge. Entropik will have an economic incentive to tie up with schools and colleges and collect and commodify as much student data as possible. A company that builds its AI technologies, purportedly intelligent and emotionally perceptive ones, without mentioning the phrase privacy or confidentiality in their Privacy policies, strives on large and diverse student datasets. In such contexts, corporations need to balance the pecuniary interest of the stakeholder against the public values of privacy and other associated fundamental rights. Such contradicting loyalties threaten and strain the fiduciary relationship between a corporation and the public. As Professor Zittrain suggests, a fiduciary must subordinate its private interests over its clients if the two conflict.[525] However, a business model like Entropik, built around capturing large datasets to understand emotional behaviour, collecting sensitive personally identifiable information upon which building a portrait of a student and selling it to school authorities, runs contradictory to users' privacy interests. Khan and Pozen refer to such contradictions as a '*perpetual conflict of interest*' between the company and the public values.[526]

One question one must remember while evaluating the fiduciary concept is whether the economic incentive structure is reconciled with public values. The legal analysis shown above, by way of the Entropik Tech example, leads us to a situation where a difference between the traditional

[524] Bajpai, H, The Rise of Emotiveillance? Emotion AI and Ed-Tech in India, *The Bastion*, October 12, 2020, Available at https://thebastion.co.in/covid-19/the-rise-of-emotiveillance-emotion-ai-and-ed-tech-in-india/.
[525] Zittrain, J., Mark Zuckerberg Can Still Fix This Mess. *The New York Times*, 7th April, 2018, Available at https://www.nytimes.com/2018/04/07/opinion/sunday/zuckerberg-facebook-privacy-congress.html.
[526] Supra note, 515 pg. 512.

fiduciary and modern-day information fiduciary relationships can be seen. While the former relationships put the users' interest in the centre, it is implausible for the latter to prioritise public communities and their values, due to their particular business model. Professor Julie Cohen puts the said difference succinctly:

> *"Traditional fiduciaries operated on small scales and at human rhythms for a reason. The fiduciary construct implies a mutual encounter predicated on the knowability of human beings as human beings, with mutually intelligible desires and needs. The information fiduciaries proposal abstracts speed, immanence automaticity, and scale away from that encounter and then assumes they never mattered in the first place."*[527]

Expanding on knowability of human beings, Khan and Pozen draws on their second critique of the phrase information fiduciaries.[528] The second critique looks at two nuanced features of a fiduciary relationship: a) expertise, b) personal exposure.[529] Traditional relationships like that of a doctor possess professional skills and expertise, which are sought by a fiduciary. Also, there is an information asymmetry in a doctor-patient relationship and the power is in the hands of the doctor, which can lead to exposure of personal information. Thus, the question is whether both features can be distinguished between traditional and information fiduciaries.

It is not to say that companies/fiduciaries like Entropik Tech do not provide expert or individualised judgements to its beneficiaries like students or school authorities. School authorities are provided with a complete behavioural profile of students, including learning engagement levels, which means a better and personalised output for a student for improvement. Also, to create an Emotional AI application, it would have a team of experts in product design, data analytics, software engineers and marketing to provide a personalised experience. Furthermore, just like doctors and lawyers need to learn sensitive details of the individual to provide a personalised service, Entropik Tech also leans on the sensitive attributes of a student to provide meaningful outputs. Thus, on the surface, both expertise and personal exposure, traditional and information fiduciaries stand at par. It means that the nature and structure of traditional and information fiduciary relationships are the same. However, as Julie Cohen states, the small-scale business

[527] Cohen, J. E. (2013). What privacy is for. *Harvard law review*, *126*(7), 1904-1933.
[528] Though Khan and Pozen draw a comparison between traditional fiduciary relationships and Facebook - a social media company, we exhibit (in)differences between corporations and traditional fiduciaries.
[529] Both the nuanced features have been enunciated in previous scholarships of Balkin and Frankel. Refer to, Balkin, information fiduciaries, supra note 467 and Frankel, Fiduciary Law, Supra note 501.

structure and meaningful competition in traditional fiduciary relationships make it distinctive from corporate fiduciary relationships.[530] Frankel has also supported the view by stating that the competition between doctors and lawyers provides an economic reason to safeguard the interests of the beneficiaries.[531] Between school authorities or students and Entropik, the latter is in a monopolistic position of extracting data from students - who have nowhere else to go unless leaving the school altogether - further compounding the vulnerability in terms of invading students' privacy. Thus, Balkin's proposal obscures the power imbalance in a commercial data fiduciary relationship that distinguishes it from traditional fiduciaries.

1.4.2. GUARDIAN DATA FIDUCIARIES

The previous drafts on Data Protection had a distinct category of data fiduciaries for the protection of data subjects under eighteen years of age. Such data fiduciaries, called as guardian data fiduciaries, are defined as entities that a) operate commercial websites or online services directed at children or b) process large volumes of personal data of children. The definition is marred with two broad challenges. *First*, it includes schools, EdTech companies, gaming companies etc. under one category, which is problematic due to their differing goals and responsibilities. *Second*, its usage of ambiguous words like 'online services' or 'large volumes' makes the definition unclear. How much processing will amount to large volume, whether websites operating under public private partnership amount to commercial websites, or how to differentiate between a GDF providing world history lessons one which is providing online proctoring service as both are 'online services', or are websites/services targeting, directing the children are different than the ones which are attractive to children, are some of the questions that remain unanswered in the Bill. Due to such unclarity of words, painting all fiduciaries as GDF is arbitrary and unreasonable.

The Bill also prohibits GDF from 'profiling, tracking or behaviourally monitoring, or direct targeted advertising at children'.[532] The question about the difficulty to enforce or implement these measures remains, especially when the objective of the Bill talks about fostering growth of digital products and services. We can analyse the conflict between fostering digital economy and informational privacy through an online service, YouTube, that is increasingly being used as an

[530] C. Julie, Scaling Trust and Other Fictions, *Law and Political Economy*, 29th May 2019. Available at, https://lpeproject.org/blog/scaling-trust-and-other-fictions/.
[531] Frankel, Supra note 501.
[532] See section 16 of the Personal Data Protection Bill, 2019. Available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

educational tool in Indian schools.[533] YouTube, to comply with the US federal children privacy law made changes to its policies. In 2020, targeted ads were restricted from children's centric videos, comments were disabled and community features like sending push notifications were also discontinued. Post rollout of such features, YouTube has agreed that it led to a significant business impact due to reduced ad-revenue.[534] Thus, introduction of privacy by default features, to safeguard children's privacy rights might conflict with the government's objective of fostering digital products and services.

Furthermore, online services like YouTube use machine learning technology to differentiate the videos made for kids and those made for adults. Presently, it is opaque about what kind of data is used by YouTube to differentiate videos meant for kids. It is difficult to gauge the intention of YouTube showcasing a particular video to children. YouTube comes with a default autoplay feature that allows videos to play automatically based on Youtube's algorithms.[535] The default autoplay setting amounts to a manipulative design that can potentially nudge children to remain online, view only particular channels (i.e. trick into making certain choices losing personal autonomy) and place the onus on the child to stop their viewing activity. In features such as autoplay, the notion of consent becomes further meaningless. In the case of GDF, in order to deliver a service to a child, consent of a parent is required. Though, a parent can provide a consent to a YouTube Kids platform, or even to particular videos. But it is impractical for a guardian to provide consent to endless streaming videos delivered to children via algorithmic engineering. Though there are certain settings/controls like timer, preselection of certain channels to bypass the said challenges, they are not by default features.

It would be worthy talking about a regulation that has found mention in various legislations around the world meant for protecting children's privacy rights: '*Age Verification*'. Previously drafted

[533] K. Shyna, Teachers turning YouTube into education platform amid lockdown, *Indian Express*, April 26, 2020, Available at: https://indianexpress.com/article/education/teachers-turning-youtube-into-education-platform-amid-lockdown-and-how-you-can-do-it-too-6371382/. Similar products were also unveiled by Google in 2021, especially in areas where internet infrastructure is dismal or discontinuous. Google also boasts providing services in regional languages contributing to its wider reach. With AI and ML powered products, it provides personalised experience and contribute to child's learning outcomes. For more details refer to, https://indianexpress.com/article/education/sending-assignments-in-form-of-images-accessing-edtech-in-offline-mode-google-rolls-out-india-specific-features-7192998/.

[534] Julia Alexander, The Verge, Jan 6, 2020, Available at: https://www.theverge.com/2020/1/6/21051465/youtube-coppa-children-content-gaming-toys-monetization-ads.

[535]H. Rebecca, YouTube's kids app has a rabbit hole problem, Vox, May 12, 2021, Available at, https://www.vox.com/recode/22412232/youtube-kids-autoplay.

legislations in India also mandate data fiduciaries, specifically GDF, to verify the age of the child and then obtain consent from their guardian. Since children are highly vulnerable to harms associated with the Internet, there has been a global call to making the Internet a safer space by offering age verification measures and restricting the processing of children data. Under the Indian legislation, though the scope is unclear, the obligations apply to any company, not necessarily a social media platform, which targets/directs any product, design feature, or setting that processes personal data of children.[536] As per the 2019 Bill, there are several factors to be taken into account while deciding the measures for age verification, like, volume of data being processed, proportion of data being that of a child, and possibility of the harm arising out of processing of personal data. Similar provisions can also be seen in jurisdictions like the USA[537], China[538] and UK[539], and at a global level[540]. Such measures are not specific to data protection and privacy in India, rather seem to have been borrowed from regulations concerning Pornography on social media[541] and digital media ethics.[542]

Though the above legislations use the phrase '*Age verification*' it has been interchangeably used alongside Age estimation and Age Identification methods. A UK-based organisation, working on children privacy rights, uses a collective term '*Age Assurance Methods*' encompassing Identification Methods (which obtain the true identity of the user), Age Verification methods (which verifies the exact age of the user) and Age Estimation Methods (which estimate the age of the user).[543] There has been an analysis of the advantages and disadvantages of each of the above methods that have been analysed on several parameters like Privacy-Friendliness, Usability,

[536] It is necessary to distinguish between a social media platform from business as for the former, the Indian legislation specifies a distinct category of fiduciaries called as significant data fiduciaries. However, the latter can be an online platform but also a company that designs, develops or deploys AI technologies specifically processing children's data. Thus, the latter encompasses a wider set of entities.
[537] Kids Internet Design and Safety Act and Children and Teens Online Privacy Protection Act.
[538] China has restricted children's usage of online gaming apps: https://www.cnbc.com/2021/08/30/china-to-ban-kids-fromplaying-online-games-for-more-than-three-hours-per-week.html.
[539] UK ICO's Age Appropriate Design Code of Practice for online services, Online Harms Bill.
[540] 43rd Closed Session of the Global Privacy Assembly, Adopted Resolution on children's digital rights, October 2021 https://globalprivacyassembly.org/wp-content/uploads/2021/10/20211025-GPA-Resolution-Childrens-Digital-Rights-FinalAdopted.pdf.
[541] Rajya Sabha Ad-Hoc Committee Report on Pornography on Social media and its effect on children and the society as a whole.
[542] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[543] 5RightsFoundation. (2021, March). But how do they know it is a child? Age Assurance in the Digital World. Retrieved August 04, 2021, from 5Rights Foundation: https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf.

Inclusiveness, Accuracy and Feasibility.[544] However, it is necessary to note that such parameters are dependent on subjective understanding of the children and parents.

In India, different legislations have different ages of child between 0-18. While some recognise persons under 12 or 14 as children, some identify persons as 16 or 18 as children. Such categorisations of children in age-groups are based on the level of risk/harm children might face due to a particular legislation. Thus, a legislation based on its scope, purpose and objectives equate maturity and put a person under a category of childhood or adulthood. However, a one size fit all approach might not work in the context of harms emanating from different kinds of technologies and platforms. It is due to the technicalities of a technology and objectives of the platform that can restrict or protect the rights and opportunities of a child. Using a single definition of adulthood or maturity levels prevent a child from availing the benefits of a technology or a platform which can be detrimental to the development and overall well-being of a child. Also, there might be some cases where a child is more capacitated in understanding risks of a technology or the platform than the parent diluting the requirement of seeking the consent of the parent after age-assuring the child.

The entire discussion of Information and Guardian Data fiduciaries highlight the flaws in the concept of 'fiduciary' in data protection and privacy context. It also lays out the reasons behind the power, control and information asymmetry between the data fiduciaries and data subjects. The previous discussion on Aadhaar also showcased the opaqueness with which a variety of actors operate in the digital realm. In order to address the said concerns and create, in Nissenbaum terms, norms of 'appropriateness' and 'distribution', the next chapter will provide fairness and transparency principles that should be strengthened in the Indian data protection legislation.

CONCLUSION

The recently unveiled National Education Policy looks at education as a "*single organic continuum from re-school to higher education*".[545] It uses key phrases while underlining the objective of the policy, like, "changing the educational landscape", "new and far-sighted policy", "providing high-

[544] Briefing Paper, Global Technological Developments in Age Verification and Age Estimation, CUTS International, Available at, https://cuts-ccier.org/pdf/bp-global-technological-developments-in-age-verification-and-age-estimation.pdf.
[545] National Education Policy 2020, Ministry of Human Resource Development, Government of India.

quality education to all" and "preparing the youth to meet present and future challenges". All the said objectives are driven by the goals of "access, equity, quality, affordability and accountability". Upon reading the objective and the guiding goals, they focus more on the outcomes - of achieving universal coverage, affordability, inclusivity, and accountability - rather than devising policy around what would be needed to achieve such outcomes. For instance, the twenty-third goal of NEP is '*Technology Use and Integration*' where the government moots the idea of establishing an autonomous body, the National Educational Teaching Forum (NETF), to "*facilitate decision-making on the induction, deployment and use of technology*", leaving the idea to delve upon designing and development of such technologies. NEP lacks both attention and intention to follow a bottom-up approach of first building policies around designing and moving up the ladder to deploy such technologies. It should also be considered that policy around integrating technology with education is bereft of any conversations around Data Protection Bill - or its predecessors - and its lacunae.

To support the NEP, there is a plethora of research, as indicated above and across chapters, focusing on the harms and risks associated with the usage of technologies, however devoid of an action plan to tackle the challenges. To address datafication of children in schools requires regulations that go beyond a broad data protection legislation. Undoubtedly, data protection legislation can set up the broad contours of privacy mechanisms, however, this chapter shows the incompleteness of such legislation, globally. The discussion in the current and previous chapters boil down to, a) How should courts examine a given technology and resist its design, development and deployment, b) How can the norm of appropriateness and distribution be made effective in a school context that safeguard personal information of students from invasive AI-based technologies and Aadhaar, c) How can data subjects rights be strengthened that provide them more power to have control over their information that reduced power asymmetry and safeguard informational and decisional privacy and, d) Whether the role of parents should be reduced in certain contexts while increasing child's participation to exercise rights, provide consent and seek grievance redressal in privacy claims?

Though, by now it might be perceived that law is incapable of regulating such technologies, but, fostering greater collaboration and interdisciplinary research can tackle the issue of privacy and the above raised questions in an AI age. In an attempt to stitch together a draft sectoral legislation and policy solutions, the sixth and the last chapter will return to various legal scholarships. The sixth chapter will browse through tort, environmental, contract and corporate laws, signalling that

effective legal norms are already present in other legal disciplines. Such laws already possess data governance solutions to preserve data protection and privacy and counter technical difficulties but need a revamp in order to suit the digital age. Rather than providing a list of solutions, the next chapter will focus on four broad principles - Fairness, Accountability, Transparency and Equity - which will form the bedrock of safeguarding Informational and Decisional privacy of children. Because if the model is accurate, it is devoid of all the abovementioned harms, thereby protecting individual privacy rights.

CHAPTER 7

REGULATION OF AI TECHNOLOGIES: SETTING THE REGULATORY AND LEGISLATIVE AGENDA

Successive periods of industrial revolutions have given way to either concentration of market power through self-regulatory techniques or intrusion of the State into the market by government regulation or legislative measures. When manufacturing and engineering processes advanced in the first industrial revolution, regulations were made around such technologies' health and safety risks. The second industrial revolution witnessed engineering marvels and the development of faster means of communication. Most regulations were reactive and made to prevent risks or allocate the resources equitably (such as auctioning airwaves for radio). The third industrial revolution, also closer to the present A.I. revolution, saw the advent of computing and the Internet, which started with the market regulating itself, i.e., self-regulation, until the risks of cyberspace became known recently. Finally, the fourth industrial revolution is upon us, creating disruptive technologies, i.e., which substitute or overturn traditional business models, for which regulation is being sought at national and international levels.

Julia Black and Andrew Murray identify and model six stages through which a product or service passes and where there is a scope for building regulation.[546] The six stages include: a) Proof of theoretical concept, b) Development of the prototype, c) Construction of the distribution system of the product, 4) Licensing of the product, 5) Commercial Exploitation, and 6) Reactive regulation. Though each product or service does not need to pass through all these stages, the authors justify that each of these stages is common to all the industrial revolutions gone by. For instance, if we look at 'horse carriages,' the U.K. has the oldest legislation regulating such road vehicles. The legislation was made to regulate carriages on highways/roads that are shared public resources. The intention of this legislation spilt over to the second industrial revolution when powered motor vehicles came into existence. Apart from the shared public resource, the purpose of regulation was also to safeguard the public from the dangers of the motor vehicle (like accidents, vehicle insurance, provisioning seat belts, pollution control measures, etc.). Both horse carriage and motor vehicles will follow the model outlined above without going through the fourth stage, i.e., licensing. Globally, the licensing regime looks different and is generally limited to the technologies

[546] Black, J., & Murray, A. D. (2019). Regulating AI and machine learning: setting the regulatory agenda. *European journal of law and technology*, *10*(3).

that came during the third industrial revolution, i.e., hazardous chemicals, radio, computing technologies, aerospace, nuclear energy, pharmaceuticals, and nuclear and atomic energy. Some of the said sectors follow a compulsory licensing model, whereas other sectors have sector-specific exceptions. For example, due to the scarcity of airwaves, the governments globally regulated radio communications by auctioning them to specific providers. This regulation also spilt over to cyberspace and the 5G era. Therefore, not all technologies pass through the fourth stage and are commercially available.

The socio-legal and political context of the times and circumstances often dictate which regulation will exist. For instance, the cyberspace sector saw regulations in multiple phases, continuing even now. Cyberspace began with a libertarian ethos, primarily initiated by John Perry Barlow.[547] As their movement came to be known, the cyber-libertarians believed that cyberspace is limitless and borderless - outside the purview of international law. They argued that cyberspace is not analogous to maritime, air, or space routes and comprises domain names, protocols, and data. Their argument also involves a claim of extraterritorial jurisdiction, as it cannot be governed under a particular sovereign nation due to cyberspace's unlimited characteristics. In contrast, previous technologies like shipping, space, or aircraft created platforms for shared transparency and responsibility, but it was due to limited shipping routes, orbital paths, and aviation corridors, respectively. In essence, they claimed that the Internet could not be governed, which also became the title of a seminal piece written by David Johnson and David Post - also cyber libertarians - in a question format, i.e., And How Shall the Net be Governed?[548]. They reiterated Barlow's argument that cyberspace is chaotic, and no answers exist to attributing liability. During this first phase, the governments, while embarking on the glow of faster connectivity and adhering to the claims of digital libertarians, could not see the future risks that such self-regulation can pose.

Soon, cyberspace risks took multiple forms, evolving continuously, like copyright infringement, abuse of personal data, online fraud, threats, hate speech, and acts of violence. The second phase saw a rise in reactive regulations primarily led by a group that came to be known as Digital Realists led by people like Cass Sunstein, Jack Goldsmith, Tim Wu, Lawrence Lessig, and others.

[547] John Perry Barlow, who also later founded the Electronic Frontier Foundation was known to be at one end of the extreme of cyber libertarians or digital libertarians who declared a movement to fight government control over cyberspace. At the other end of the extreme were Froomkin, Post, and Johnson who gave reasoned, formal, and ordered reasonings against state control.

[548] Johnson, D. R., & Post, D. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review*, 1367-1402.

The school of digital realism points out that the rule of law for every human endeavour can and should be extended to cyberspace. Jack Goldsmith, in his paper '*Against Cyberanarchy*,' draw no difference between the 'real' and 'cyber' space and calls for traditional governmental regulations. He sees law as a governmental device that can be used across territories to regulate harms that emanate from both 'spaces.' He goes on to make a valid argument that the mode through which the harm emanates is irrelevant. This school understood that the changing technologies would challenge governmental regulations, and the law must adapt. Such a 'wait and see' approach also became a significant limitation of the school as digital realists championed reactive regulatory measures. Another limitation of the school was that it emphasised law but needed to answer more practical questions as to what an effective law would look like.

Amidst the tussle between the first phase of Cyberlibertarians, where self-regulation was given primacy, and the second phase of digital realists, which marked the beginning of state control, came a taxonomy that lies at the centre of the two schools of thought. 'Code is Law' propounded by Lawrence Lessig, and to a smaller extent, Joel Reidenberg came as the third and the present phase of cyberspace regulation. Lessig asserts that four' modalities of constraint can regulate human behaviour': a) Law, which is enforced via sanction; b) Markets that operate per demand, supply, and price; c) social norms that thrive on relationships and human interactions and d) architecture, meaning the operative environment. Lessig argues that 'architecture' is an essential and effective modality to regulate cyberspace. In cyberspace, the architecture consists of hardware and software, i.e., the 'Code' written by a handful of players, and which determines the actions of the users. Thus, code is the law of cyberspace, which controls the bodies and acts as a contract between the user and the digital sphere. By providing the taxonomy, Lessig provides a solution for the ever-changing technology environment by exposing the code to scrutiny. However, Lessig needs to answer what effective regulatory strategy can be modelled. The starting point, though, lies in his paper 'Code is Law' that rather than the government exerting complete control over the code, a tailored intervention should be balanced between security and innovation.

The experience from the different phases of Internet Regulation serves as a warning. It provides a gaping hole that needs to be filled in the context of the fourth industrial revolution technologies. A regulatory strategy that can be a potential '*tailored intervention*' is the Responsive Regulation approach which resembles Lawrence Lessig's modality of '*architecture*.' Both advocate for understanding the environment in which technology operates and then building a structure

conducive to that environment.[549] It can be helpful to bring responsive regulation to A.I. and biometric technologies installed in schools and the risks they emanate, i.e., data protection and privacy. Such a regulatory approach will also juxtapose well with Helen Nissenbaum's Theory of Contextual Integrity (as discussed in the second chapter) - that advocates privacy and data protection to be contextual to the people, communities, and institutions that shape its meaning. The regulation of A.I. and its risks can be located within the '*Discourse of the Indian School System*,' set out in the third and fourth chapters, which outline:

1. How technology mediates in a school setting.
2. How the school administration and other stakeholders handle privacy and data protection issues.
3. What are the consequences of such handling on the students and teachers?

While the previous chapters outline the '*architecture*' of a space where A.I. technologies are being deployed, the last chapter will create - in Lessig's terms - a '*Law*' that takes the form of a Responsive regulation.

Before we start formulating a responsive regulation, it is necessary to mention that this idea is not novel in the Indian context. A research organisation has referred it to the Committee of Experts, which drafted the first report on what data protection legislation should look like in India.[550] Still, there lies a novelty in applying the approach to specific nuances of a sector and building the contours of sector-specific legislation. As previous chapters clearly outline, children are one of the most vulnerable sections of society that deserve transparent, fair, accountable, and equitable regulation. This chapter attempts to carve out and achieve the aims of sector-specific legislation.

In the said attempt, **Part A** provides a Rule of Law based test that can guide the data protection regulator and judiciary to evaluate any AI-based or biometric technologies before deployment. The rule of law will be tested on the primary three grounds adopted globally, i.e., legality, necessity, and proportionality. **Part B** will dive deep into the Fairness, Accountability, Transparency, and Equity principle (FATE) that safeguards children's Right to privacy and data protection. The FATE approach will move beyond the traditional space of data protection law. It

[549] For more details on Responsive Regulation, see Ayres, I., & Braithwaite, J. (1995). *Responsive regulation: Transcending the deregulation debate*. Oxford University Press, USA.

[550] Responses dated 31 January 2018 to the "White Paper of the Committee of Experts on a Data Protection Framework for India" dated 27 November 2017 (White Paper) released by the Ministry of Electronics and Information Technology (MeitY), Dvara Research, Available at https://www.dvara.com/research/blog/wp-content/uploads/2018/02/Response-to-White-Paper-Public-Consultation-Dvara-Research.pdf.

will corroborate the machine learning lifecycle (Design, Development, and Deployment) showcased in the previous chapter to regulate privacy risks at each stage. For instance, it will talk about how the lack of an effective auditing ecosystem in the Indian education sector poses risks to the data protection and privacy of children in the age of A.I. Therefore, Part B explores the existing regulatory harms, exposes its limitations in the changing technological landscape, and then enunciates a responsive regulation. Lastly, **Part C** will expand on broader issues that certainly impact children's privacy risks but impact the entire data ecosystem. The paper concludes with a deeper understanding of what a 'tailored intervention' can look like and what specific roles the market and the State must take to safeguard children's privacy rights in the A.I. age.

PART A - RULE OF LAW-BASED REGULATION

Justice Kennedy, in his address at the 20th Sultan Azlan Shah Law Lecture stated that "*Although I cannot recall hearing the phrase the rule of law in common usage when attending college and law school, half a century ago, it has deep roots*".[551] The 2004 Report of the UN Secretary-General, entitled *The Rule of Law and Transitional Justice in Conflict and Post-Conflict Societies,* identified certain substantive and procedural principles that constitute the rule of law. Procedural principles include, for example, that laws and regulations must hold supremacy, be publicly promulgated, accessible to all, and enforced equally by an independent judiciary. The substantive principles included that laws must conform to international human rights law standards and require the removal of arbitrariness. Before the 2004 U.N. report, the rule of law was enunciated by an English philosopher, A.V. Dicey, in 1897 and sixty years later by an Austrian economist and political theorist, F.A. Hayek, in their book The Constitution of Liberty. Their conceptualisation has influenced and been embedded in various democratic constitutions worldwide. Both formulated the rule of law in three concepts, i.e., firstly, there should be the supremacy of the law that dissolves arbitrary power or broad discretion of the authority to the government; second, all should be equally subjected to that law, and third, that law is the consequence of the rights of the individuals as defined and enforced by the courts. Both were also influenced by the writings of John Locke, specifically the Second Treatise of the Government, where he states:

[551] Anthony M. Kennedy, Assoc. Justice, U.S. Supreme Court, Address at the 20th Sultan Azlan Shah Law Lecture: Written Constitutions and the Common Law Tradition (Aug. 10, 2006) Available at http://www.sultanazlanshah.com/pdf/2011%20Book /SAS_Lecture_20.pdf.

> *"[T]he end of law is not to abolish or restrain, but to preserve and enlarge freedom: for in all the states of created beings capable of laws, where there is no law, there is no freedom: for liberty is, to be free from restraint and violence from others; which cannot be, where there is no law: but freedom is not, as we are told, a liberty for every man to do what he lists: (for who could be free when every other man's humour might domineer over him?) but a liberty to dispose of, and order as he lists, his person, actions, possessions, and his whole property, within the allowance of those laws under which he is, and therein not to be subject to the arbitrary will of another, but freely follow his own.")*[552]

Distilling from such definitions, some scholars and legal practitioners have tried to articulate the tenets of the rule of law. For instance, Robert A. Stein, in his paper, establishes eight principles of the rule of law, namely, 1) Superiority of the law, 2) Separation of powers, 3) Law should be known and predictable, 4) Equal Application of law, 5) Just Law, 6) Robust and accessible enforcement, 7) Enforcement by an independent judiciary, and 8) Right to Participate in the development of laws.[553] The examination of each tenet may be helpful for this thesis/chapter (like the independence of the judiciary, separation of powers, etc.) and extend beyond the scope of privacy and data protection. It should be borne in mind that any technology must be examined against the said rule of law principles. It is because the broader purpose of the rule of law is society's welfare, which also resembles the objective and intention of why a particular legislation is drafted.[554]

The phrase has also been developed through constitutional adjudication, yielding precedents but aptly formulated in the context of privacy in the *Puttaswamy* judgement. The *Puttaswamy* judgement referred to an earlier precedent *Golak Nath v. State of Punjab*. C.J. Subba Rao dwelt on the rule of law's purpose and stated that "*every authority constituted by the Constitution is subject to it and functions within its parameters*."[555] Similarly, the judgement notes another

[552] Locke J., SECOND TREATISE OF GOVERNMENT 32 (C.B. Macpherson ed., Hackett Publ'g Co. 1980) (1690).
[553] Stein, R. A. (2019). What exactly is the rule of law? *Hous. L. Rev.*, *57*, 185.
[554] Pound, R. (1908). *Mechanical Jurisprudence,* Columbia University Press, Roscoe Pound in Mechanical Jurisprudence states that *law must be judged by the result it achieves, and not by the niceties of its internal structure*; Cardozo, B. N., & Kaufman, A. L. (2010). *The nature of the judicial process*. Quid Pro Books, according to Benjamin Cardozo *a law that misses its aim of the welfare of society cannot permanently justify its existence*; Llewellyn, K. N. (1930). Some realism about realism--responding to Dean Pound. *Harv. L. Rev.*, *44*, 1222, *Llewellyn conceptualises law as a means to a social end…so that any part needs constantly to be examined for its purpose and for its effect.*
[555] 1967 AIR 1643.

landmark precedent *ADM Jabalpur v. Shivakant Shukla* which stated that a threat or invasion of personal life and liberty leads to suspension of the rule of law.[556] Such a statement was also made in the context that arbitrary or uncontrolled power might lead to state encroachment. Therefore, regulated freedom is the bulwark of the rule of law that can only be curtailed in cases of necessity and proportionality. Justice Khanna's opinion in the same judgement evoked a sense of the rule of law that fits well with the usage of A.I. technologies in schools and the impact it has on the rule of law:

> "*The impact upon the individual of the massive and comprehensive powers of preventive detention with which the administrative officers are armed has to be cushioned with legal safeguards against arbitrary deprivation of personal liberty if the premises of the rule of law is not to lose its content and become meaningless…*".[557]

Thus, in India's legal jurisprudence, the rule of law has been interpreted to deal with the new developments and accepts an expansive reading of personal liberty and freedom, which also placed the Right to Privacy as a fundamental right under the same gamut. The *Puttaswamy* judgement recognises the balance between state interests and the protection of liberty and freedom. It mandates the State to formulate a robust regime that fulfils the three-fold requirements of legality, necessity, and proportionality to maintain the rule of law. [558] It is against India's brush with the regime of personal liberty and the constitutional vigilance that safeguarded it, with which the A.I. technologies should be tested before their design, development, and deployment. The rule of law is still ongoing and will evolve with technological changes. However, it must also be resilient to allow the future generation and their technologies to adapt to its content, basic features, and principles.

1.1. Legality

Using A.I. technologies in schools will entail a more significant collection of personally identifiable information amounting to privacy risks. Such a risk to the fundamental Right to privacy should be prescribed by law, which is publicly accessible. Such a law cannot be in the form of an ordinance as it is promulgated by the Executive, thus demanding legislative scrutiny.[559] A similar view has

[556] (1976) 2 SCC 521.
[557] Ibid, para 574.
[558] Puttaswamy, Supra 267, pg. 254, pp, 180, Part S.
[559] *ADM Jabalpur v. Shivakant Shukla*, (1976) 2 SCC 521. Justice Bhagwati's opinion at p. 701, pp. 459.

been taken by courts globally, owing to the inherent danger of abuse in any monitoring system capable of surveillance.[560] In the Indian case, a broader piece of data protection legislation is currently tabled before the Parliament and, therefore, not a law. There are also specific regulations/manuals published by education boards, as discussed in the third chapter, which cannot be deemed as law. Thus, India needs more legislation explicitly allowing the installation of A.I. technologies in schools. Even if we assume specific state regulations to be a law, they need to meet three requirements: a) the legislature should pass them, and not by the Executive;[561] b) they should be accessible and foreseeable – this is to ensure the quality of the law, and c) it should be clear and precise – to limit the scope of the discretion. The U.K.[562] and the European Court of Human Rights[563] also recognise this three-prong test of legality. Since the Indian jurisdiction fails the first element of the test, it is meaningless to discuss the latter two; however, if examined, they can prove helpful in future legislation's remit.

The second element of legality is the quality of the law in terms of the richness of the content of the law and its accessibility and foreseeability. The intention behind the inclusion of the element is to allow citizens to understand the law and seek grievance redressal. If the content of the law is sufficiently explicit, i.e., is not vague and arbitrary, it would provide an opportunity for the citizens to foresee the harms and risks emanating from such technologies.[564] While it does not mean that the legislation incorporates a definitive list of harms or risks, a government rationale for introducing such technologies through legislation might prevent arbitrary interference with the fundamental rights of the citizens.[565] On foreseeability, the EctHR in *Zakharov v. Russia* observed that:

> "*The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures*".[566]

[560] For instance, *Escher et al. v. Brazil*, 2009 Inter-American Court of Human Rights, which stipulated that monitoring technologies should be deployed based on precise legislation with clear, detailed rules.
[561] *State of Madhya Pradesh v. Thakur Bharat Singh* 1967 AIR 1170, *Kharak Singh v. State of U.P. AIR 1963 SC 1295*, *Bijou Emmanuel v. State of Kerala*, 3 SCC 615 (1986), paras 16, 19.
[562] *Sunday Times v. U.K.*, App No 6538/74, A/30, [1979] ECHR 1, (1979).
[563] *Otto-Preminger-Institut v. Austria*, App. No. 13470/87, Eur. Ct. H.R. (1994).
[564] *Uzun v. Germany*, 53 EHRR 852 (2010), and *Perry v. U.K.*, 39 EHRR 3, (2004), para 45.
[565] *Malone v. U.K*.[1984] ECHR 10.
[566] *Zakharov v. Russia*, Application No. 14881/03, ECHR.

Legality's third and final element is legislation's clarity and specificness. The law can prevent its abuse by limiting the scope of the legislation, attributing powers to a specific regulator, and limiting the scope of discretion.[567] According to Victoria Aitken, "*quality of law is dependent on the substantive content of the legislation, form, and language of legislation, operation of legislation and processes for producing and implementing legislation*".[568] Vanterpool also echoes Aitken stating that legislation should be precise and effective in achieving the intended outcomes and be proportionate to its stated object and purpose.[569] Vanterpool also equates with Jean-Clause Piris's explanation of clarity, who describes it as appropriateness, adequacy, and precision of legislative provisions that can achieve a desired aim through predictable and equitable implementation.[570]

1.2. Proportionality & Necessity

Once legislation is in place that allows the design, development, and deployment of technologies in schools and satisfies the test of legality, i.e., is clear, concise, and precise, it still needs to pass the test of proportionality. The Indian courts in *Modern Dental College and Research Centre and Ors v. State of M.P.* adopted the four-pronged proportionality test from Chief Justice of Israel Aharon Barak's book "*Proportionality: Constitutional Rights and Their Limitation*."[571] While delivering the judgement in Modern Dental College, Justice Sikri also referred to the proportionality test in the Canadian Jurisprudence framed by Dickson C.J. in *R v. Oakes*.[572] Both Israel and Canadian jurisprudence frame the proportionality test according to four components: a) The action should have a proper purpose (legitimacy), b) The action taken is inextricably connected to the desired purpose (rationality and reasonableness), c) The action is utmost necessary, and no alternative measure can achieve the same purpose (necessity) and d) Proper relation between the social benefits of limiting a fundamental right and the objective that needs to be achieved (balancing test). This four-part test is settled law in India following a straightforward reading of *Puttaswamy I and II* (known as the Aadhaar Judgements, where the proportionality test was put to the test against a technology that captures biometrics). This sub-section intends to draw upon learnings from the Aadhaar judgement and test it against the deployment of

[567] *Vukota-Bojic v. Switzerland*, ECHR 899, (2016) 73, 77; *Piechowicz v. Poland*, ECHR 689, (2012) para 212.
[568] Aitken, V. E. (2013). An exposition of legislative quality and its relevance for effective development. *ProLaw Student Journal*, *2*, 1-43.
[569] Vanterpool, V. (2007). A critical look at achieving quality in legislation. *Eur. JL Reform*, *9*, 167.
[570] Ibid at 170.
[571] *Modern Dental College*, (2016) 7 SCC 353.
[572] *R v. Oakes*, 1986 SCC 6.

technologies in schools. The section also devotes particular emphasis to the third prong, i.e., a necessity, as it has been considered the heart and soul of the proportionality test.[573]

1.2.1. Legitimacy

All the purposes for which biometric technologies are deployed must correspond to a legitimate aim identified in the valid law. Due to the absence of a law that explicitly permits the usage of such technologies in schools, we can closely examine the Indian constitution, significantly Articles 19 and 21, which safeguard freedom of speech and expression and the Right to privacy. Article 19(2) specifies specific legitimate aims when a right can be circumvented by the State, like, national security, public safety, sovereignty and integrity of India, prevention of disorder or crime, protection of health or morals, or for the protection of rights and freedoms of others. One can also find a similar exception under Article 8(2) of ECHR. The European Court of Human Rights has interpreted the word '*legitimate aim*' as one which should be '*necessary in a democratic society*', i.e., that answers a pressing social need.[574] The burden of proof is on the State to demonstrate the legitimate aim of the measure.

To satisfy the test of a legitimate aim, the State must show that goal is necessary to be achieved in society and is aimed at solving a legitimate problem. For instance, in *R v. Oakes*, the Court adjudicated legislation to criminalise drug trafficking. The Court considered evidence that showed an increase in drug trafficking and that similar legislation in other countries has been able to tackle the problem. In *Puttaswamy*, while considering the constitutionality of collecting biometrics for a digital I.D., the State claimed it is necessary to address fraud and leakages in the public distribution system. The judgement has been criticised as it allowed the State to continue the Digital ID program even when it could neither prove a direct connection between creating a biometric identity and plugging leaks in the welfare system nor could it give ample evidence of countries where such a measure has proven success.

It is essential to mention the Digital ID program's legitimate aim as it is one of the data sources for the partnership between the Telangana Government and Microsoft who aggregate that data with other publicly available datasets to monitor a student's entire school journey to predict the risk of that student dropping out of school. Therefore, the question arises when the legitimate aim of the program is to plug leakages in the public distribution system; how is the biometric data

[573] Hogg, P. W. (2007). *The constitutional law of Canada*. Thomson Carswell.
[574] *Von Hannover v. Germany*, Application No. 59320/00, ECtHR.

being used by a private player to predict the drop-out rate of students? This phenomenon is known as function creep, where a technology established to serve a purpose is deployed to serve other purposes without any checks and balances. The question becomes more apparent if one reads the object and purpose of the Aadhaar Act. It states, "*It is an act to provide for, as a good governance, efficient, transparent, and targeted delivery of subsidies, benefits, and services… to individuals residing in India through assigning unique identity numbers to such individuals*". It would be hard to place the objective of predicting the drop-out rate as a subsidy, benefit, or service to any individual within their respective meanings in the Aadhaar Act.[575] Even if this could be proven as a legitimate aim, the digital I.D. data cannot be shared and accessed by a private entity as established in *Canara Bank*.[576] Therefore, it would be fair to say that collecting children's biometrics and its aggregation with other datasets under the Digital ID program of Aadhaar does not pass the legitimate aim test.

Now, let us look at the CCTV cameras context. The safety and security of children have been the government's aim, coupled with other legitimate aims like the prevention of bullying and corporal punishment.[577] As highlighted in the third chapter, state governments across India have provided similar aims and objectives for installing GPS location-based technology services, RFID enabled Smart ID cards. Due to rising incidents of grievous crimes in schools across the country, the government might be able to prove the goal is legitimate and necessary to be achieved in a democratic society in cases where CCTV cameras or GPS systems, or RFID tags are used to prevent the occurrence of a crime. Still, such usage of cameras might fail the legitimacy test as the legitimate aim of safety and security is mentioned in a circular released by the Central Board of Secondary Education. An executive circular bereft of any legislative scrutiny differs from a Surveillance Camera Code of Practice in the U.K., which was laid before the Parliament for members to discuss, amend and update.[578] The code is much more detailed than a circular, as it

---

[575] "*Benefit*" means any advantage, gift, reward, relief, or payment, in cash or kind, provided to an individual or a group of individuals and includes such other benefits as may be notified by the Central Government;) "*Service*" means any provision, facility, utility or any other assistance provided in any form to an individual or a group of individuals and includes such other services as may be notified by the Central Government; "*Subsidy*" means any form of aid, support, grant, subvention, or appropriation, in cash or kind, to an individual or a group of individuals and includes such other subsidies as may be notified by the Central Government.

[576] *District Registrar and Collector, Hyderabad v. Canara Bank*, (2005) 1 SCC 496.

[577] Central Board of Secondary Education, Circular Number, 19/2017, Safety of Children in Schools, Available at: https://www.cbse.gov.in/cbsenew/Examination_Circular/2017/16_CIRCULAR.pdf.

[578] Guidance by Biometrics and Surveillance Camera Commissioner, Surveillance Camera CoP, https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-ccamera-code-of-practice-accessible-version.

guides the appropriate and effective use of surveillance camera systems. Principle one of the code states that the person deploying the CCTV system must consider the end user's requirements regarding whether the captured images by a camera will be used for the legitimate aim, and if yes, by whom. Ideally, if the legitimate is safety and security or preventing a crime, the end users would be school authorities, and law enforcement agencies, and the criminal justice system. For the technological solution to be legitimate, the law must specify the actors who can capture and use the images. The law should be precise in its scope, extent, and applicability as to

1. whether both State and private actors can use the images,
2. under what circumstances to use, and
3. for which purposes the said actors can use.

Due to the absence of such a law, the deployment of CCTV cameras for the safety and security of children will not pass the legitimate aim test.

Similar arguments can be drawn for justifying fingerprint-based attendance systems for students and teachers whose legitimate aim is to curb teacher absenteeism and truancy. For instance, while launching the biometric-based attendance system in Gujarat in partnership with Facebook and Microsoft, the government claimed there would be no more '*manipulation*.'[579] It is a similar objective as emphasised by the European Parliament while digitalising the European Parliament's Central Attendance Register (CAR) for its Members. The benefit of the proposed solution over the current manual CAR system was to prevent fraud and manipulation.[580] While no law currently permits the collection of fingerprints in Gujarat schools, it should consider the European Data Protection Supervisor's (EDPS) comments in the E.U. case while framing future regulations. In the CAR case, the EDPS considered the European Parliament Rules of Procedure Article 12, which states rules around attestation of attendance. It allows for an electronic attestation of a

[579] Ritu Sharma, Facial Recognition Attendance System in Gujarat, Indian Express, Available at: https://indianexpress.com/article/education/facial-recognition-attendance-system-it-is-fool-proof-has-no-scope-for-manipulation-says-education-secretary-5925570/.

[580] EDPS Opinion on the use of a computerised system by the European Parliament, Available at: https://edps.europa.eu/system/files/2021-03/21-03-29_edps_opinion_ep_computerised_system_biometrics_en.pdf. Some of the other benefits provided were that a member can give attendance even if it forgets the badge or any other identifying documents. It was also stipulated that prevention of fraud and manipulation is key to the members as they should lead by example and exercise honesty, transparency and accountability in their duties.

member's attendance in place of their signature. The EDPS concluded that electronic attestation does not imply the collection of fingerprints. For the technological solution to pass the legitimacy test, the Parliament's internal rules should be adapted to "*clearly and specifically indicate that biometric registration shall be used as a rule to attest attendance*."[581] To conclude, it is again fair to state that installing a fingerprint attendance system will not pass the legitimate aim test.

Another technology currently being deployed in classrooms is emotional A.I. products. Such products can be used for taking attendance and tracking students' activities by capturing individuals' movements and expressions. Such products are sold by convincing the school authorities that the product will measure cognitive learning by "*monitoring two metrics - attention and engagement*."[582] Though it is an upcoming technology in India, and therefore devoid of any explicit legislation, businesses are selling it intending to install such technologies to curb cheating during online or physical exams, enabling better online assessment that can capture children's psychometric, cognitive, and technical abilities, and measure a child's attentiveness in the classroom.[583] Ministry of Electronics and Information Technology (MEITY), in its blog, uses Gartner's report to laud the usage of such technologies in the education sector as it helps to enable child's attention levels and track learning disabilities.[584] If future legislation uses the stated objectives as a legitimate aim, it could not pass the legitimacy test. It would be hard for the government to provide evidence of such technologies' success in other countries, especially when countries prohibit or classify AI-based emotion technologies as 'high-risk' applications. For instance, UNHRC, in its 2021 Resolution: '*Right to Privacy in the digital age*, notes more safeguards for emotion recognition applications.[585] Similarly, CoE calls for a strict ban on such technologies in education and the workplace.[586] In 2021, the EDPS and EDPB issued a joint notification declaring the use of Emotion AI products as highly undesirable and finding that they should be prohibited.[587] The proposed EU AI Act also classifies emotion recognition as a high-

[581] Ibid, p 5.
[582] Bajpai, H., The Rise of Emotiveillance? Emotion AI and Ed-Tech in India, October 12, 2020, Available at https://thebastion.co.in/covid-19/the-rise-of-emotiveillance-emotion-ai-and-ed-tech-in-india/.
[583] Refer to Chapter III.
[584] Balaji S., *EIGHT areas where emotion AI is high-impact and high-value*, Feb 01, 2021, Available at, https://indiaai.gov.in/article/eight-areas-where-emotion-ai-is-high-impact-and-high-value.
[585] United Nations General Assembly (2021) Resolution adopted by the Human Rights Council on October 2021, 48/4, Right to privacy in the digital age.
[586] Council of Europe, Consultative Committee of the Convention for protecting individuals concerning the automatic processing of personal data, Convention 108: Guidelines on facial recognition, 2021.
[587] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a regulation of the European Parliament and the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021.

risk application.[588] The UNCRC General Comment No. 25 also rejected one of the legitimate aims of deploying such technologies that advocate strengthened engagement between the teacher and student and between learners.[589] To conclude, the government could not pass the legitimate aim test. Before installing such high-risk technological solutions, it should take cues from other countries, especially the EU.

1.2.2. Rationality/Reasonableness

The second test of proportionality involves that reasonable means should be sought to achieve the desired measure or objective. The measures should be reasonable and reasonable to the legitimate aim sought to be achieved. The Indian Supreme Court established a settled position on reasonableness in *Laxmi Khandsari v. State of U.P.,* where it made clear that the Court must consider the "*nature and circumstances of the case, the objective that the measure sought to achieve, infringed right, the purpose of the restriction imposed, the extent and urgency of the evil sought to be remedied*."[590] The Court also considered that though it is hard to apply such considerations to each case at hand, it still pointed out that each Court should look towards the Directive Principles of the State Policy (DPSP) outlined in the Indian constitution.[591] It is because DPSPs are drafted to establish social control leading to an egalitarian society to establish a framework of welfare state within the constitution.[592]

In our thesis context, Article 39(f) states, "*The state shall direct its policy towards securing that children are given opportunities and facilities to develop healthily, and conditions of freedom and dignity and that childhood and youth are protected against exploitation and exploitation moral and material abandonment*." Though there is limited jurisprudence on Article 39(f) and lesser on specifically Biometric surveillance and DPSP, it has been briefly taken into cognisance by the

[588] European Commission, Proposal for a Regulation laying down harmonised rules on artificial intelligence, 21st April 2021.
[589] UNCRC (United Nations Convention on the Rights of the Child) (2021). General Comment No. 25 (2021) on children's rights in relation to the digital environment.
[590] (1981) 2 SCC 600.
[591] The directive principles of state policy have been drafted to embody the concept of a welfare state, stated by the Supreme Court in *Keshavnanda Bharti v. the State of Kerala* (1973) 4 SCC 225; However, DPSB do not confer any enforceable right, and their alleged breach does not invalidate a law, nor does it entitle a citizen to complain of its violation (*Deep Chand v. State of U.P.*, AIR 1959 SC 648). However, according to the same court, decisions have pointed out that DPSP has a positive effect too. It has been asked to harmoniously construct DPSP and fundamental rights together (*Grihakalyan v. Union of India*, 1991 1 SCC 611). It has also been stated in *Chandra Bhavan v. State of Mysore* AIR 1970 SC 2042 *or Lingappa v. State of Maharashtra* AIR 1985 SC 389 that legislation enacted to implement the directive principles should be upheld, as far as possible, without tinkering with the basic feature of the constitution.
[592] *Laxmi Khandsari v. State of U.P.*, 1981 AIR 873.

Delhi High Court. In *Rajesh Kumar v. State (Govt. of NCT of Delhi)*, the installation of CCTV cameras in Child Care institutions (CCIs) was in question. The Court opines that the safety and security of the children are of primary importance and recognises that there should be "wide awake" security guards assigned each night along with security personnel for emergencies. The Court, emphasising children's Right to privacy and confidentiality, states that measures like installing CCTV cameras should be a last resort as they would make a CCI look like a prison or detention centre.

Suppose CCTV installation in classrooms is to be evaluated. In that case, it might fail the test of reasonableness as classrooms are supervised mainly by teachers and class monitors, who are responsible for maintaining the safety and security of children. It is essential to note that a CCTV installed in the classroom, and one installed in playgrounds or classroom corridors needs to be treated separately. The safety and security risks posed to children at different points in a school, and the level of intrusiveness at each point should be balanced against the objective sought, like deterring theft/disruptive behaviour/bullying and identifying unauthorised visitors. If such a balancing exercise is not undertaken, a school can easily justify using CCTVs in classrooms and toilets that are much more prone to bullying and other crimes.[593]

Second, data protection legislation globally treats biometrics as highly sensitive data, including the present Indian data protection Bill. It is because, as shown in the fourth chapter of the thesis, biometrics are immutable, innate, and distinctive to an individual. In the cases of children, it also keeps continuously changing during the pre-teen and teenage years. Third, there is a high information asymmetry between a student and the school about the reasons for fingerprint collection, where they will be stored, and how they will be used, i.e., sharing, accessing, and aggregating the school's policies. Fourth, fingerprints are proven to reveal data on gender and genetic disorders with 90% accuracy. It could open room for systemic gender-based discrimination in a country like India, especially where a student belongs to the LGBTQ+ community.[594] Thus, fingerprints reveal more than what is often consented for without the

[593] Big Brother Watch captured students' voices in UK schools on the use of CCTV in schools where children find the usage of cameras in classrooms, toilets, and other sensitive places/or places where there is already a teacher supervision, to be intrusive. https://www.bbc.co.uk/newsround/19567142.
[594] Dantcheva, A., Elia, P., & Ross, A. (2015). What else does your biometric data reveal? A survey on soft biometrics. *IEEE Transactions on Information Forensics and Security*, *11*(3), 441-467; Zhai, X., & Renzong, Q. (2010). The status quo and ethical governance in biometrics in mainland China. In *Ethics and Policy of Biometrics: Third International Conference on Ethics and Policy of Biometrics and International Data Sharing, ICEB 2010, Hong Kong, January 4-5, 2010. Revised Papers* (pp. 127-137).

knowledge of both the giver and the receiver. Using biometric technologies like fingerprints allows the school administration to enter a child's beyond school life, which is not only an evident invasion of privacy but, at a societal level, can increase mistrust between a school administration and the child. Fifth, even if the dangers of the technologies are ignored, the school administration must prove that there was an effective consultation with parents and children before deploying such technologies.[595]

The case of RFID or smart I.D. cards for children might yield a different conclusion than biometric technologies and CCTV cameras due to the purpose for which the former is used. Smart ID cards have a unique identifier that enables access to other databases for verifying a child's authenticity, thus providing access to the facility for which the I.D. cards are being issued, i.e., to avail meals, to enter the school premises, or availing books in the library. Apart from providing access, RFID also has the potential to track a child's movements within and outside the school campus, given that they are also installed in school buses. RFID technology is much more advanced than the one used in the Travel smartcards like Oyster. Oystercard collects information about people's journeys by tapping upon entry and exit. However, the new RFID tech sends bursts of radio waves to the linked database almost every second. It is also far more accurate than traditional global positioning systems (GPS), which can nail down to the exact inches. Thus, RFID's reasonableness can be evaluated based on the purpose it wants to achieve. If RFID is used for access purposes, the school administration will have to prove if there has been a history of impersonation, such as students marking attendance on behalf of others or unauthorised persons entering the buses/availing meals, etc. To prevent fraud, the school must justify and document the fraud likelihood assessment as the main driver for processing student data. However, if the technology is used for tracking each child's movement, the bar would be much higher as personally identifiable data is being collected continuously. The use of RFID systems on children is tortious under a conceptualisation of privacy, i.e., seclusion and the Right to be let alone (as conceptualised in the second chapter).[596] There are certain moments and locations within a campus when a child would have a reasonable expectation of privacy, especially during lunch

Springer Berlin Heidelberg; Similar concerns have been raised in the US consumer industry where they are classified into categories based on race, ethnicity, and income levels, Schneider B (2015), The Hidden Battles to collect your data and control your world. New York, W.W. Norton.

[595] Such consultations should provide a complete and accurate description of how this technology ill be deployed including a) name of the company whom the tender has been given, b) data sharing, accessing, retention, and security policies and c) rules regarding grievance redressal system.

[596] Stein, S. G. (2007). Where Will Consumers Find Privacy Protection from RFIDs? A Case for Federal Legislation. *Duke L. & Tech. Rev.*, *6*, 1.

times, playgrounds, and after school gets over, in their buses.[597] A child might not be comfortable letting the school administration know about its timeline of conversations with a particular teacher or student. However, the intrusiveness of RFID technology allows such monitoring. Details regarding when a child meets their friend, why a child meets a particular staff member, and why the child is currently in the laboratory room rather than in the library are issues that can be solved using other less intrusive means, as discussed in the third test of necessity.

The last technology for consideration is the emotional recognition technology that works through the Facial Action Coding system (FACS) - works when an individual's face is in front of the system and, henceforth, a biometric system. It runs by capturing the emotions of a given face by factoring in the body position, body language, movement of the muscles, and facial features. The first question to be proven in the Court to prove its reasonability should be why a teacher could not understand the response of their classroom. Second, does the depiction of each child's emotions the same in every situation? It should be considered here that the patterns of muscle movement and coordination are at a formative stage, especially among children but also among young adults, thus making FACS prone to wrong conclusions.[598] Third, it would be challenging to legitimise the collection of emotions - another sensitive data point - and balance against the child's best interests. Fourth, emotional recognition technologies do not acknowledge the cultural differences that influence the mood depicted on the face. People of different genders and classes participating in the same class might have very different lived environments and circumstances, showing on their faces.[599] While specific technical characteristics like Fairness and Transparency of such systems would be discussed in Part B of the chapter, it should be briefly noted here that if such systems are designed in Western countries, they might not be able to adapt to the real-

[597] The thesis appreciates that the concept of 'reasonable expectation of privacy' is contentious globally. For example, in the ECHR context, the ECtHR found in *Lopez v. Ribalda* that, as workers were in a store where they were bound to meet others, there was no reasonable expectation of privacy. ECtHR has on other occasions accepted that there was an expectation of privacy even on the public street or other quasi-public places (*Peck, von Hannover 1*), where the purpose of the data collection doesn't serve a legitimate aim. Another interesting case to look at from this perspective is *Antovic and Mirkovic v Montenegro*, which concerned the privacy of lecturers in a university amphitheater (the Court found that their filming did not serve the stated aim of protecting student safety). The Indian courts could use the existing global and national jurisprudence to address the emerging technologies impact on right to privacy.

[598] Barrett, L. F., Adolphs, R., Marsella, S., Martinez, A. M., & Pollak, S. D. (2019). Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements. *Psychological science in the public interest*, *20*(1), 1-68.

[599] A similar point was acknowledged by El Kaliouby in a World Economic Forum article. Computers Can Now Read Your Emotions. Here's Why That s Not as Scary as It Sounds, World Economic Forum. See more at Hutchinson, B., Denton, E., Mitchell, M., & Gebru, T. (2019). Detecting bias with generative counterfactual face attribute augmentation.

world cultural conditions of India and how children react. Thus, the choice of technology should also factor in the reasonableness of technology deployment. The IEEE, a standard-setting organisation that has worked on Ethically Aligned Design, has also cautioned against using such systems as they cannot assess an individual's internal emotions and experience.[600]

1.2.3. Necessity

The third stage of the proportionality test is a more fact-based test to determine if a less intrusive measure could have been deployed to achieve the legitimate aim. Such an analysis is done to identify the measure that has the least harmful effect while achieving the goal. Such a least intrusive measure should be equally able to achieve the purpose effectively, as any other measure would. The test was wrongfully applied in the Aadhaar judgement without the State being asked to show if it has considered other alternative measures. Instead, on the petitioners' inability to showcase suggestive measures, the Court deemed the passage of the said test. Another element not given importance in the majority judgement of the Aadhaar case was the I.D. system's '*structure and design*.' In technological cases, the means adopted to store, share, or access data might not pass the least intrusive test. For instance, the dissenting opinion of Justice Chandrachud in the Aadhaar case referred to the storage of Aadhaar biometric details in a centralised database. On account of the risks posed to the security of such details, it was asked if there was no other alternative measure available, like federated databases. The Court referred to the CJEU case of *Michael Schwarz v. Stadt Bochum*, where the regulation was said to be disproportionate as it did not provide for any other form or method of storing fingerprints apart from a centralised storage mechanism.[601]

Although the Aadhaar judgement suffered from several legal casualties, it laid down a test for the necessary facet of proportionality analysis. Using a formulation found in the work of Professor David Bilchitz, the majority bench of the Aadhaar judgement observed that the necessity test requires:

> *"First, a list of possible alternatives to the measure employed by the government must be identified. Secondly, the effectiveness of these measures must be determined individually,*

[600] Affective Computing The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, Available at, https://standards.ieee.org/wp-content/uploads/import/documents/other/ead1e_affective_computing.pdf.
[601] [2013] CJEU C- 291/12.

> *i.e., whether they can realise the governmental objectives real and substantially. Thirdly, the impact of each of the alternative measures on the right in question should be mapped."*[602]

In the context of CCTV, it would be challenging for the State to prove that CCTV has been an effective tool for safety and security, especially when there are several contrary pieces of evidence. An ethnographic study in two American secondary schools found that children find it unnecessary to use security strategies like cameras.[603] Another study in U.K. secondary schools proves that even if CCTV is installed for safety and security, children tend to frame strategies for evading, resisting, and negotiating with such technological solutions.[604] The State would need to make strong arguments as to why traditional monitoring practices like class monitors, teacher observation, attendance registers, and surprise searches (of lockers, desks, bags, and clothes) is not effective method of maintaining discipline and the time demands for the introduction of such invasive and intrusive technology. Similar holds for emotion recognition technologies deployed for understanding students' learning engagement levels. It needs to be proven in courts if traditional examinations, progress reports, and teacher observation methods are not adequate alternative measures to understand children's experiences and perceptions. Even after the abovesaid arguments, if CCTV's necessity is proven, it would be impossible to justify the necessity of CCTV videos being live streamed with parents. Such a step significantly increases the level of anxiety about being observed by parents (including the possibility of being viewed by the parents of other children), chilling the fundamental rights of a child.

Similar arguments can be made against installing fingerprint-based biometric technology in schools, mainly for attendance. Such measures would prove challenging to comply with the necessity test. The school's first need to furnish an impact assessment of a physical attendance register (a measure being substituted with the biometric system) and whether it has posed any limitations earlier. Each school using a fingerprint-based attendance system should outline the number of fraud/manipulation incidents that have occurred previously. There is a burden of proof

---

[602] Bhandari, V., & Lahiri, K. (2020). The surveillance state, privacy, and criminal investigation in India: Possible futures in a post-*Puttaswamy* world. *U. Oxford Hum. Rights. Hub J.*, 15.
[603] Bracy, N. L. (2011). Student perceptions of high-security school environments. *Youth & Society*, *43*(1), 365-395.
[604] McCahill, M., & Finn, R. (2010). The social impact of surveillance in three UK schools: Angels, devils, and teen mums. *Surveillance & Society*, *7*(3/4), 273-289; Popular strategies among children include switching, distorting, blocking, and masking, as discussed in Hope, A. (2010). Student resistance to the surveillance curriculum. *International Studies in Sociology of Education*, *20*(4), 319-334.

on the schools to show if they deployed any less intrusive solutions to uncover such fraud. Is such fraud happening among all age groups or only done by teenage children? Schools might claim that the fingerprint attendance system saves time and provides real-time data recording, saving manual inefficiencies. However, it is something for the Court to determine if saving time and providing convenience outweighs the collection of sensitive personal details of children.

1.2.4. Balancing Test

The fourth and final proportionality test is also called proportionality *stricto sensu*. The balancing test requires a measure to be balanced based on the benefits and the risks it poses. If the measure can be justified on the scales of human dignity and one that produces social benefits in a democratic society, it would balance with the rights invaded. For instance, in the famous case of Internet Shutdowns in Kashmir, the Supreme Court balanced the marginal costs versus the marginal benefits of a shutdown.[605] The government aimed to curb anti-social activities through social media. However, the Court asked the State if there had been no anti-national activities before the advent of the Internet. Further, the Court also considered the uproar by the people of Kashmir, resulting in protests and demonstrations against the government and shaking the law-and-order situation, which was sought to be maintained in the first place. It is coupled with the loss of jobs, reduced trade, and hampering education that relies on the Internet. The Court thus rejected the internet shutdown order as such has a reversing effect on the democratic society.

Considering the overall objectives of the Aadhaar project on society, Justice Chandrachud, in his dissenting opinion, declared the Aadhaar project unconstitutional based on its design flaws and stated:

> "*Our quest for technology should not be oblivious to the country's real problems: social exclusion, impoverishment, and marginalisation. The Aadhaar project suffers from crucial design flaws that impact its structural probity…. The Aadhaar project has failed to account for and remedy the flaws in its framework and design, leading to serious exclusion issues. The dignity and rights of individuals cannot be based on algorithms or probabilities…. Above all, the design of the project will be compliant with the structural due process only if it's responsive to deficiencies, accountable to the beneficiaries, and places the burden of ensuring that the benefits reach the marginalised, on the state and its agencies*."

[605] *Anuradha Bhasin v. Union of India, Writ Petition (Civil) No. 1031/2019.*

We must examine the impact of CCTV and other technologies at a societal level to prove their (dis)proportionality. Whether CCTVs are used for security, fingerprints for attendance, and RFIDs for access control, a power differential exists between the school administration and children. There needs to be more information about technology's positioning, technical abilities, and objectives regarding their usage and who has access to the video/audio/biometrics.[606] A study done in Israeli schools shows that the power disparity between children and adults is more profound as a child is younger. Such disparity has been shown to correspond to a lower consciousness of one's rights. For instance, if a child is under a panoptic gaze since early childhood, it can completely lose the idea of resistance - overt or subverted - leading to the normalisation of surveillance.[607] The children and teachers have previously expressed that the student-teacher relationship or the peer relationships are marked by personal secrets, jokes, manifestations of love, conversations, laughs, etc., that hold no meaning in the age of CCTVs in the classrooms as it tramples dignity, intimacy and 'right to be alone.'[608] Another study notes that children have noted that they are now not allowed to commit mistakes, learn from them and take responsibility. Technologies, rather than emphasising creating an environment that nurtures growth, are producing docile bodies.[609] Thus, the societal harms of producing children with negligible critical thinking skills who cannot make informed decisions outweigh the educational, evidentiary, and security benefits of the technologies deployed in a classroom. Similarly, studies have also shown a power disparity between teachers and principals. The latter's controlling tendencies using technologies as a surveillance tool lead to increased stress, low motivation, and low social status among teachers.[610] It is also important to note the spatial and temporal nature of CCTV that CCTVs are often targeted at students. However, teachers are caught on camera, amounting to function creep, thus further contributing to complexities within schools' social fabric. Such a function creep technically impossible in fingerprints used for attendance or RFIDs enabling access control.

---

[606] Perry-Hazan, L., & Birnhack, M. (2018). The hidden human rights curriculum of surveillance cameras in schools: Due process, privacy, and trust. *Cambridge Journal of Education*, *48*(1), 47-64.
[607] Almog, S., & Perry-Hazan, L. (2011). The ability to claim and the opportunity to imagine: Rights consciousness and the education of ultra-Orthodox girls. *JL & Educ.*, *40*, 273.
[608] Birnhack, M., Perry-Hazan, L., & German Ben-Hayun, S. (2018). CCTV surveillance in primary schools: normalisation, resistance, and children's privacy consciousness. *Oxford Review of Education*, *44*(2), 204-220.
[609] Warnick, B. (2007). Surveillance cameras in schools: An ethical analysis. *Harvard Educational Review*, *77*(3), 317-343.
[610] Eyal, O., & Roth, G. (2011). Principals' leadership and teachers' motivation: Self- determination theory analysis. *Journal of educational administration*, *49*(3), 256-275.

While judging the proportionality of intrusive technologies, the courts must question how far it should be allowed, if at all. For instance, in the case of GPS, the technology gives a child's real-time location to parents' phones. Such devices are used for tracking school buses and when a child goes on camping trips or school excursions. Experts have called it psychologically damaging for parents to have constant access to their children's whereabouts. It not only leads to increased anxiety for children but parents too. As has been written before, parents are under pressure, created by school authorities and other parents, to perform their obligations diligently.[611] One of the core obligations includes attentive love that has three dimensions attached to it: *first* is that love is not essential, rather parents should react to children's vulnerability; second, contribute to the child's intellectual development and *third*, make sure that the child adjusts to the societal norms.[612] The media, businesses, and school administrations often capture the first dimension to push technology forward on children. Using the first dimension, the technologies are sold to achieve the second and third dimensions, thus completely changing the dynamics of parental responsibility.[613] Thus, understanding the societal implications of such technologies is necessary for the courts to do an injustice to the proportionality analysis.

Emotional recognition technologies' exact usage and intended goal differ with every use case. For instance, the European Commission did propose new safety requirements for vehicles with drowsiness detection. Such technology serves the social goal of saving human lives, as it is expected in the E.U. that by 2038 such technologies can save more than 25,000 lives and help safeguard 140,000 severe injuries.[614] Such narrow use of A.I.s can also be impactful and serve a rational purpose. However, in the case of schools, it does not merely provide a prompt like in vehicles. They impact the results of a child's teacher-student relationship, possibly leading to a change in the child's emotional State. Rather than serving the goal of increased engagement, it could backfire.

Post our four-pronged analysis of various technologies deployed in schools, they should only be able to pass the proportionality analysis test in courts. Though based on no legal basis, the

[611] Fahlquist, J. N., & Van de Poel, I. (2012). Technology and parental responsibility: the case of the V-chip. *Science and engineering ethics*, *18*, 285-300.
[612] Ibid, p., 292.
[613] Fahlquist, J. N. (2016). Ethical concerns of using GPS to track children. In *Surveillance Futures* (pp. 122-131). Routledge.
[614] Krier, S., '*Facing affect recognition',* 18th September 2020, Asia society.

proportionality test fails at the first stage. However, it was still necessary to show that even after a legal basis, such technologies, if used in a classroom setting, would fail at the second, third, third, and fourth stages. Often it is not the legal tests alone that can prove a measure's legitimacy, necessity, and reasonableness. Instead, the courts would need to rely on psychological, education, social, economic, and technical experts to conduct an interdisciplinary inquiry into a government measure to arrive at the measure's proportionality. Though the above analysis used psychological and education-based evidence to prove that such technologies are disproportionate, it was bereft of any technical and socio-economic analysis. As highlighted in the previous chapter, each stage of the machine learning lifecycle poses dangers of exclusion, bias, and profiling, thus hampering users' privacy. Thus, it is essential to build a principal-based regulation that explicates the deployment of such technologies ethically and responsibly in a situation where the law allows its usage. While technologies fail to pass the rule of law-based tests, the thesis proactively suggests principle-based regulations for circumstances where technology is already deployed.

PART B - PRINCIPLES-BASED REGULATION

Any technology is admissible if deployed ethically and responsibly. Part B is an attempt to provide the ethical and responsible principles that can be used by government and industry groups to design, develop and deploy emerging technology in schools in a responsible manner. The courts can use such principles to test the proportionality of present and future technologies, and the legislators could insert the principles into the data protection legislation. Without a principle-based regulation, there are no standards/benchmarks for developing and deploying technological systems that could risk students' *Right to Privacy*'. While certain principles should be considered when designing or procuring an algorithmic system (like fairness and transparency), others become useful when deployed (like accountability and equity). However, these principles are not practicable in water-tight compartments but can be applied depending on the nuances and circumstances in which a system operates.

By enacting principles as legal obligations in a data protection law, a legislator could incorporate '*privacy by design*' or '*data protection by design*' (DPbD) at each stage of the technological system. Article 25 of the GDPR also obliges the controller to take measures for specific technological contexts and embed data protection and privacy principles into each context:

> *"Having regard to state of the art and the cost of the implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this regulation and ensure the protection of the rights of the data subject."*

Article 25 also suggests certain DPbD principles in the form of '*technical and organisation measures and procedures'* like pseudonymisation, purpose limitation, and data minimisation. However, they are not an inclusive list as the article allows the data controller to apply the measures contextually, as the term '*appropriate*' implies. The thesis delineates Article 25 by a) Providing a framework for the word '*processing*' in the previous chapter by outlining a machine learning lifecycle divided into three parts, i.e., design, development, and deployment. Though GDPR defines processing as a set of operations performed on personal data ranging from collection and storage to disclosure and dissemination but is devoid of any clear framework, and through the current chapter will b) Stipulate different technical and organisational measures that the data controller can deploy during each stage of the lifecycle to achieve fairness, transparency, accountability, and equity. One thing to note before delving into the principles is that lacunaes highlighted in the GDPR below should not be equated to it being an inadequate legal framework. The below stated FATE principles highlight some missing points in the GDPR and provide a framework that both GDPR and the Indian data protection legislation should incorporate to safeguard privacy at the design, development and deploying stages of an AI technology.

2.1. Fairness

Fairness as a principle is tightly connected to the Right to privacy, but only sometimes in explicit terms. Fairness, whether in machine learning or the legal domain, has been interpreted through the lens of discrimination, protected classes or groups, Affirmative action, or Disparate treatment.[615] For instance, the Indian supreme court tied privacy with discrimination in the case of *Suresh Kumar Koushal v. NAZ Foundation (Koushal)*, in which the court stated that discrimination against individuals based on sexual orientation is deeply offensive to the dignity and self-worth of the individual.[616] Herein, the court focuses on the dignity and autonomy

[615] On the legal compatibility of fairness definitions. Fairness and discrimination find mentioning in the Indian constitutional jurisprudence with respect to Article 15, however this chapter covers the said concept through the lens of data protection law and privacy.
[616] *Puttaswamy*, Supra 267, pg. 124.

conception of privacy to protect an individual's sexual orientation. While discussing the rationale of *Koushal* in *Puttaswamy*, the court further noted that any act causing discrimination is constitutionally impermissible due to its chilling effect on exercising fundamental rights. Article 21, which recognises the Right to privacy as a fundamental right, states, "*No person shall be deprived of life and personal liberty unless the procedure is established by law*". The phrase procedure established by law has been interpreted to mean that the procedure must be fair, just, and reasonable. Although presently, the test of whether a procedure is fair, just, and reasonable is done through the proportionality analysis, as articulated in Part A, it is essential to outline what fairness entails concerning emerging technologies.

Technology-led education through data-driven artificial intelligence technologies operates in an ecosystem traditionally patterned with systemic inequalities. As shown in Chapter 3, students face discrimination based on colour, gender identity, religion, caste, and age, which forms part of everyday school life in India. Such discrimination pervades the minds of students, and teachers, who are often data collectors for a particular technology. It has also been proven in the previous chapter that such data collectors might feed incomplete, incorrect, and biased information into the technologies due to their own biases. Further, the previous chapter also noted that such technologies rely upon historical datasets that could be more accurate and need to cover the relevant input details needed for the technology to operate and provide decisions. Thus, AI technologies rely on troves of student data and have a high possibility of exacerbating inequality and discrimination, contributing to incorrect algorithmic predictions, and violating an individual's Right to privacy.

Different surveillance technologies tend to discriminate among students at different data lifecycle stages. For instance, when facial recognition-enabled CCTV cameras record a particular classroom, no disparate treatment is involved, as the entire environment is captured. Discrimination occurs when students are flagged in a video based on preconceived notions and biases, i.e. at the data processing stage. Data processing includes data annotation or labelling stage, where facial expression, speech, or movement are attributed to good or bad behaviour. It brings biases of what behaviours are good or bad in a person's eyes that might not necessarily corroborate with what a teacher or a student thinks. Thus, each tilting of the head, change in facial expressions, style of speech, and movement of eyelids can be comprehended differently, yielding wrong predictions about a child's behaviour, thus exacerbating discrimination. It would not be far-fetched to say that a similar kind of technology would also be able to discriminate in the future

based on religion. Though there is no record of it happening in a classroom, records of facial recognition-enabled CCTV cameras disproportionately targeting Muslims have attracted the eyes globally.[617] A technology deployed by biased human minds in a stratified society would further exacerbate inequality and discrimination, thus contributing to unfairness. Such forms of discrimination violate individuals' autonomy and dignity to freely decide and express their thoughts, thus infringing their privacy.

While in the case of cameras, the discrimination occurs mainly at the data processing stage, in particular technologies, it can creep in at the first stage of data collection. In the case of an artificial intelligence technology predicting the drop-out rate of students, how would it decide the factors of students dropping out? A singular case of a student dropping out is complex because several individual, societal, and school factors contribute to the decision.[618] The child's socioeconomic status, stress and anxiety levels, availability of school infrastructure, parents' job transfer, quality of teachers, choice of friends, student fighting, overall grades, or discipline and punishment record all can result in the chances of a student dropping out. While creating a list of potential factors for dropping out is possible, it could only be an exhaustive list, meaning that some factors could not be identified, thereby not factoring as input variables for a technology. Based on incomplete input variables, the technology cannot establish causal evidence of a student dropping out, leading to wrong predictions. Such inaccurate predictions might prove discriminatory based on gender. Girls tend to drop out due to several societal factors, like early marriage, the non-availability of girl toilets, or low grades due to extensive household work. Incorrect input data generating wrong predictions or outcomes lead to tailored teacher interventions that a child might not need and simultaneously exclude a child who might want such interventions. Thus, such technologies for predicting drop-out levels violate children's Right to privacy by collecting non-education-related personal data to input into the model. They also breach their autonomy by singling out their choices.

[617] Sarita, S., '*Indian Police use facial recognition to persecute Muslims and other marginalised communities*', 11th October 2022, Available at https://www.codastory.com/authoritarian-tech/india-police-facial-recognition/.

[618] Balfanz, R., & Legters, N. (2004). Locating the Dropout Crisis. Which High Schools Produce the Nation's Dropouts? Where Are They Located? Who Attends Them? Report 70. *Center for Research on the Education of Students Placed at Risk CRESPAR*.

One technical and organisational measure that the data controller can deploy is a) Data Protection Impact Assessments (DPIAs) to make technologies fair, privacy respecting, and non-discriminatory.

2.1.1. Data Protection Impact Assessments

Fairness is a crucial principle of the GDPR framework that obligates the data controller to process personal data fairly and lawfully. According to ICO, if any technology infers data about an individual, the data controller should ensure that it is not discriminatory and does not produce any detrimental/adverse effects on them.[619] Under the GDPR, the principle of fairness applies before, during, and post-processing, i.e., at the design, development, and deployment stage of any given technology. The principle of fairness is not just about notifying individuals about the processing or taking their consent but also demonstrating whether the usage is proportionate and justified.

Data protection impact assessments (DPIAs) are a tool that considers the rights and freedoms of individuals and push the data controllers to consider any social or economic disadvantage of technology. So, the focus of DPIAs is not only on the Right to privacy as a standalone right but on discrimination, exclusion, exploitation, and other disadvantages that also conceptualise the Right to privacy. DPIAs are an integral part of DPbD that require data controllers to assess technological usage's legality, necessity, and proportionality. It is a handy tool for courts to seek data controllers and then conduct the proportionality analysis by scrutinising their assessment. Thus, DPIAs have the potential to provide a framework or a roadmap to the courts for providing the proportionality analysis of a given technology.

However, the question remains, what to consider at each stage of the AI lifecycle or what to document and capture to ensure fairness and non-discrimination. Article 35 of the GDPR obliges those controllers to undertake DPIAs whose processing is likely to result in a high risk to the rights and freedoms of individuals. The article enlists specific conditions under which a DPIA should be conducted, like, in cases of automated processing, including profiling, where processing is on a large scale of special categories of data, or systematic monitoring of a publicly accessible area. Thus, it would be fair to state that the instances above of technology deployment in Part A would attract Article 35's obligation. Article 35(7) takes a step further to apply a benchmark by listing the

[619] Information Commissioner's Office, Guidance on AI and Data Protection, Available at, https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/how-do-we-ensure-fairness-in-ai/.

minimum requirements of a DPIA that should be adhered to by a controller.[620] It obliges the data controller to include the purposes of the processing, legitimate interest, assessment of necessity and proportionality, assessment of risks, and the measures taken to address those risks. Section 11(2)(c) of the present Indian DPB also provides a similar but narrower requirement for conducting a DPIA.[621] Both the GDPR and Indian DPB fell short of providing an exhaustive list of how to conduct the necessity and proportionality analysis of the processing operations, how to assess the risks, or what the controller can take valid measures to address the risks. It is essential to define such requirements in legislation; otherwise, each controller would justify its assessment differently, leading to regulatory fragmentation. Further, they must be defined for each lifecycle stage and might differ with each sector.

Datasets comprise raw or unstructured data that play a critical role in the technologies deployed in a school. DPIAs can be effective if they document these dataset's motivation, creation, annotation, and usage. Documenting the characteristics of datasets at each stage of the lifecycle would help discern the reason behind technology's discriminatory predictions.[622] The said process has been used in the databases community, called '*data provenance*', and used for judging '*outcome fairness*'.[623] Timnit Gebru adopted the documentation method in AI/ML field and termed it as '*Datasheets for Datasets*'.[624] Datasheets for datasets can be effective in achieving all the principles of FATE. They can aid in locating the stage and data which is leading to exclusion or discrimination (fairness), can ensure that consumers have the data available to seek redress (accountability) efficiently, and publicising the data in public can lead to a well-informed public (transparency). Datasheets can accompany a notice for seeking contextual consent from an individual and also use for creating more datasets with similar characteristics leading to reproducibility (equity).

---

[620] UK GDPR, Article 35, Data Protection Impact Assessment, Available at https://www.legislation.gov.uk/eur/2016/679/chapter/IV/section/3.

[621] Section 11(2)(c) defines a DPIA, which means a process comprising description, purpose, assessment of harm, measures for managing the risk of harm, and such other matters concerning the processing of personal data, as may be prescribed.

[622] Information Commissioner Office, Guidance to AI and Data Protection, Annex A: Fairness in the AI Life-Cycle, Available at, https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/annex-a-fairness-in-the-ai-lifecycle/.

[623] Cheney, J., Chiticariu, L., & Tan, W. C. (2009). Provenance in databases: Why, how, and where. *Foundations and Trends® in Databases*, *1*(4), 379-474.

[624] Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Iii, H. D., & Crawford, K. (2021). Datasheets for datasets. *Communications of the ACM*, *64*(12), 86-92; The paper states that a similar method is also performed in the electronics industry where every component is accompanied by a dataset that describes its creation, usage, test results, and other information.

DPIAs incorporating datasheets for datasets can be sector-specific and outline datasets characteristics, (un)intentional misuse of data, stakeholders involved, and emerging risks and then accordingly frame solutions to address the technology and institutional architecture around it. Using the same lifecycle demonstrated in the previous chapter and juxtaposing it with *Gebru's* framework, the thesis now frames a list of indicative questions that can be used by a data controller who specifically targets or monitors children in a school.

STAGE	**QUESTIONS FOR CONDUCTING DPIA**
Problem Formulation	● What is the purpose for which the technology is being created? ● Which legitimate interest does it aim to achieve? ● Was a specific gap needed, or were any other alternative measures available? * Relevant Questions for establishing the project's lawfulness, necessity, and proportionality at the outset.
Data Collection	*If sample data is collected before the technology's deployment (like AI tool used to predict dropout rates or any other automated decision-making systems like emotion recognition tools),* ● Who collects the necessary data (teachers, students)? ● Is new data collected, or is reliance placed on the existing public datasets? If the latter name the datasets? (The answer would tell us whether there are any historical or structural biases in the dataset). ● How is it collected? Are all children's data collected, or are certain groups excluded based on protected classes? (The answer would let us know whether there is a representation or a sampling bias). ● Are all possible instances collected (like in an emotion recognition tool, instances are facial expressions, eye movements, so facial biometrics of students)? ● How are different instances captured (meaning whether CCTV is capturing live facial details or such biometrics are captured when the student is admitted into the school by clicking a photo)? The answer is whether it is a live automated collection or fed by a school administrator. If data is captured once the technology is deployed (like CCTV, fingerprint for attendance)[625], ● Who can access such datasets? ● How is such data intended to be used?

[625] Biometrics and Surveillance Camera Commissioner, Guidance Data protection impact assessments for surveillance cameras 22nd October 2018, Available at https://www.gov.uk/government/publications/data-protection-impact-assessments-for-surveillance-cameras.

	● Whether the goal/purpose could be achieved by collecting less information? (This question ensures that minimum data is collected to achieve the desired result. However, sometimes more data is needed to achieve a fairer prediction, i.e. statistical accuracy). ● Is the data confidential and thereby restricting access to a limited set of people? ● How is the consent of the child captured by the controller? ● Is it possible to identify individuals from the dataset, or is it in an aggregated and anonymised form?
Data Cleaning	● Is there a label for each instance? If yes, how is a label attributed to each instance, meaning how is it deduced that a given image showcases the emotion of anger/happiness/attentiveness/sleep, etc.? (The answer would help us know if there is a measurement bias). ● Who is responsible for labelling each instance? ● Is there any expert involved in labelling? (For instance, in the case of AI tools predicting drop-out rates, sociological and education experts should examine the existing datasets to see what information is needed to train the system. Any information missing will amount to a child's exclusion, leading to privacy loss).
Data Partitioning	● How is data split? (Highlighting how different instances of emotions are split). ● What are the reasons behind doing a 70:30 or a 50:50 data split? (The answer would tell us whether the training dataset had more data or the testing one). ● How did you prioritise and weigh different assumptions taken while splitting the dataset? (For instance, a particular input variable might be excluded or included will yield different outcomes or predictions. Thus, the said decision will lead to downstream consequences for fairness).
Model Selection	● Why is a particular model chosen for training purposes? ● Are the limitations of this particular model considered and compared with other models?
Model Training	● Does the controller consider any assumptions during training? ● Are there any proxies used to train the model? (Proxies often lead to discrimination and exclusion because proxies are collected when the variable needed to conclude is unavailable or cannot be captured. It might be the case in an AI tool to predict dropouts, where a student's stress and anxiety level is challenging to capture but is a fundamental reason behind drop-outs. A proxy in using CCTV-captured images might be used to depict stress. It would lead to bias in decision-making and is also privacy intrusive). ● How has the controller ensured a model is trained for different contexts and circumstances? (The answer would let us know whether there is any aggregation bias).[626] ● What errors were forecasted before training and steps taken to address those post outcomes? (Such an answer is necessary to maintain design fairness).
Model Deployment	● Who will maintain and update the dataset once it is in action?

[626] Aggregation bias occurs when a model is trained in a generalised manner without taking contexts into consideration.

	● Is there a contact of the maintenance person who can be contacted by the teachers, guardians, or the child in case of a data breach or to seek grievance redressal? ● If an error is detected later, what is the standard operating procedure for using the technology? ● Is there a mechanism for the third party to suggest improvements to the AI tool? ● Who is responsible for ongoing monitoring and conducting regular DPIAs? (Question is relevant to address liability at a later stage). ● Who is responsible for ensuring that the technology is not used for purposes other than its actual use? (The answer to this will tell us whether there is a function creep, also known as deployment bias).

While the previous chapter defined and depicted challenges at each stage of the lifecycle, the above table provides an exhaustive list of questions for data controllers to consider and undertake while processing the personal data of children to protect their privacy. The table also provides a roadmap for controllers, legislators, and judiciary to examine a technology by showing whether the processing is legitimate, necessary, and proportional. By outlining the questions in the above table, the thesis goes beyond *Gebru's* paper as it misses certain stages of the AI lifecycle, like data partitioning or model selection.[627] DPIAs can push the teams to go back to the questions of '*When is data enough*' and '*What data is enough*' and make changes to suit the needs of data subjects. By asking to document such questions DPIAs contribute towards fairness and transparency. The table also has the potential to reveal the risks that technology poses in different contexts and circumstances, as it uncovers all forms of bias, the stage when they occur, and who should be liable for those. DPIAs can also aid locating the stages where data drifts are occurring i.e., if the input data is being changed over time leading to incorrect predictions. Locating and mitigating drifts can prevent unnecessary data collection and motivate the data scientists to re-train the model. Such re-training helps in preventing biases producing reliable predictions, thus, indirectly, giving more control over individual's data.

2.2. Accountability

2.2.1. Algorithmic Audits

Auditing exercises can trace their origins to social sciences, anthropology, and public management.[628] Auditing has been done in such fields through field experiments, participatory

[627] Gebru, Supra 624.
[628] Vecchione, B., Levy, K., & Barocas, S. (2021). Algorithmic auditing and social justice: Lessons from the history of audit studies. In *Equity and Access in Algorithms, Mechanisms, and Optimization* (pp. 1-9).

action research (PAR), and community management. The field experiments have been conducted in a controlled setting in the real world to observe the decision-makers and their techniques. Such a study of techniques has been lauded for uncovering discrimination and biases.[629] In the AI context, field experiments can be understood as studying DPIAs of data controllers to understand their scope of activity and bring fairness and transparency. Thus, as noted above, the FATE framework needs to be water-tight, and the principles of fairness, accountability, transparency and equity flow into each other, thereby supplementing each other. The field experiments have been conducted through the PAR paradigm in which the subject is not merely treated as an informant but proactively participates in auditing. Knowledge obtained by direct participation of affected people is much better than receiving second-hand knowledge. Thus, PAR is regarded as an effective tool of social action and an enabler of full-bodied participation in a modern democracy.[630] The field of algorithmic research points out that in the absence of public participation in fairness studies - the public targeted by a particular technology - they will be an abstract exercise providing no meaningful consequence.[631] The research advocates for building community alliances that can participate in designing the algorithmic auditing approach. For instance, the data subject is allowed a right to an explanation (discussed in detail in the following sub-section) or access to seek personal records and an explanation of why specific data is being recorded. Such explanations could be handed over by data subjects to researchers or auditors to collectively identify the impact of the technologies and balance the existing information asymmetries between the data subject and the data controller.[632] Thus, PAR-based audits enable community awareness and provide information to the auditor that it might have missed, leading to increased transparency and accountability. However, such approaches are criticised if conducted in a tightly controlled environment. For instance, algorithmic research shows that sometimes audits are performed only over the training data. However, as shown in the last chapter, training data does not represent the entire population the technology uses. Thus, in a controlling environment, an audit will result in general outcomes without overseeing the real

[629] Pager, D. (2007). The use of field experiments for studies of employment discrimination: Contributions, critiques, and directions for the future. *The Annals of the American Academy of Political and Social Science*, *609*(1), 104-133.
[630] Pain, R., Whitman, G., & Milledge, D. (2011). Participatory action research toolkit. Available at https://www.durham.ac.uk/media/durham-university/research-/research-centres/social-justice-amp-community-action-centre-for/documents/toolkits-guides-and-case-studies/Participatory-Action-Research-Toolkit.pdf.
[631] Hoffman, A. L. (2022). Excerpt from Where Fairness Fails: Data, Algorithms, and the Limits of Antidiscrimination Discourse. In *Ethics of Data and Analytics* (pp. 319-328). Auerbach Publications.
[632] Mahieu, R., & Ausloos, J. (2020). Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access.

impact of the technology in a real-world environment. In the United States, it has been seen that auditors often need to disclose the choices and reasons behind auditing only a particular section or a stage of the technology.[633]

Tapping into the social sciences and algorithmic research has shown the benefits of auditing technology systems protecting data subjects' rights. However, the thesis asserts that data protection legislation should outline the auditing requirement and provide a framework for future auditors to rely on. The thesis now deep-dives into algorithm auditing and provides recommendations concerning how auditing should be done, who should do it, how auditing decisions should be disclosed, and who should audit the auditors, as providing answers to such in the Indian context can establish an effective accountability system. The Indian DPB obliges the Significant Data Fiduciaries (SDF) to appoint an independent data auditor responsible for conducting periodic audits and overseeing the compliance of the data fiduciary with various other provisions of the Bill. The meaning of 'independent' data auditor is unclear, as whether it means independent from a particular data fiduciary's contractual obligation, independent from the government/state, or a third-party orgainsation should audit the SDF. Thus, it becomes necessary for the thesis first to articulate the benefits and limitations of first, second, and third-party audits and recommend the best regulation.

First-party AI audits are now becoming common globally, with organisations with internal auditing teams, sometimes differently termed 'Responsible AI' or 'AI ethics' teams.[634] Since first-party auditors are internal, they usually have complete access to the technology they are auditing, including the datasets on which it has been trained. They, therefore, can perform responsible and continuous/periodic auditing.[635] However, first-party audits are rarely disclosed to the public resulting in their opacity. Second-party auditing is conducted by contractors, which is again an emerging field, especially with Deloitte, EY, KPMG, and PwC having establishments in India and providing auditing services. Such contractors cannot be termed independent as they are hired by an entity that intends to get audited based on a contract stipulating the auditing conditions and its disclosure policies. Thus, the auditor is bound by contractual obligations. Third-party audits are

[633] O'Neil Risk Consulting & Algorithmic Auditing, Description of Algorithmic Audit: Pre-Built Assessments, Technical Report, 2020.
[634] Facebook's Responsible AI team, Microsoft's FATE group Twitter's META team, and Google's Ethical AI and Responsible Innovation Group
[635] Costanza-Chock, S., Raji, I. D., & Buolamwini, J. (2022, June). Who Audits the Auditors? Recommendations from a field scan of the algorithmic auditing ecosystem. In *2022 ACM Conference on Fairness, Accountability, and Transparency* (pp. 1571-1583).

the most independent, as outsiders do without contractual relationships and obligations. ProPublica, The Markup, and civil society organisations like American Civil Liberties Union are the most readily cited third-party organisations. At the municipal level, New York passed the first-ever regulation that mandates third-party audits, but specific to AI tools used for hiring in employment.[636] Though an outsider's oversight of third parties is an effective mechanism, they are often challenged due to either inaccessibility of the technological system, the limits of what third parties can scope, or the lack of compensation for their work. Due to the independence and lack of bias, third-party oversight is the most efficient accountability mechanism for algorithmic auditing. However, data protection legislation needs provisions regarding a) the selection and compensation of the auditor, b) the scope and access provided to the third-party auditor to grant them legal immunity, c) accreditation and certification requirements for an auditor and d) the disclosure policies for a third-party auditor.

On Audit selection, any regulation should first clarify when the audit would be mandatory, voluntary, and complaint initiated. In the context of our thesis, where children are subjected to AI systems, where the volume and sensitivity of the data being processed are high, audits should be mandatory. There can be scenarios where there would need to be more audit resources to conduct an algorithmic audit periodically. Given the vastness of a country like India, there should be a centralised database that tracks and allows the data subject to submit a complaint and for the administrative machinery to provide its progress report. Such a method would also provide a sense of autonomy to children, who are legally represented by parents/guardians in most scenarios. The data protection policymakers can learn from the centralised Right to Information database[637] and Adverse Event Reporting Mechanisms (AERM)[638], deployed in India and the global health ecosystem. The legislation should similarly provide more clarity concerning the scope of the audit. If there is a clear mandate behind what is supposed to be audited, then the audit disclosures would be easier to translate into a clear strategy and enforceable actions. The drafters can learn from the vagueness embedded in the requirement of Environmental, Social, and Government (ESG) disclosures under the Indian Companies Act for businesses to comply.

[636] Local laws of the city of New York for the Year 2021 No. 144 to amend the administrative code of the city of New York concerning automated employment decision tools, Available at https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9&Options=Advanced&Search.
[637] Central Information Commission, Appeal and Complaint Database, https://dsscic.nic.in/online-appeal-application/onlineappealapplication.
[638] Kalaiselvan, V., Kumar, P., Mishra, P., & Singh, G. (2015). System of adverse drug reactions reporting: What, where, how, and whom to report? *Indian Journal of Critical Care Medicine*, *19*(9), 564.

The legislation calls for disclosing data on environmental protection, like climate change and greenhouse gas emissions. However, it does not specify how companies should disclose such information, i.e. in which format to benefit both the government and the business. The EU provides clarity in its Corporate Sustainability Reporting Directive (CSRD), i.e. a) information necessary to understand how sustainability matters affect them, as well as (ii) information necessary to understand the impact they have on people and the environment.[639] Such regulations that provide specificity and harmonisation in disclosures should form part of the audit scope of what specific technology components should be audited. Legislations like the Algorithmic Accountability Act also need more audit precision/scope as it asks for the Automated Decision-Making (ADM) systems to be audited. Rather than specifying ADMs, the legislation should divide the AI systems into their lifecycle's design, development, and deployment stages and refer to the abovementioned DPIAs' documentation to be audited.

On Auditor's independence, first and second-party auditors are bound by contractual obligations and non-disclosure agreements. There is an apparent conflict of interest between first, and second-party auditors and businesses/schools hiring them that can lead to compromises.[640] The auditing process could become futile if the audit targets continue hiring and compensating their auditors. Consequently, India has taken a few laudatory steps in creating a new audit regulator - the National Financial Reporting Authority (NFRA) - modelled on the Public Company Oversight Board (PCAOB) of the U.S.A. NFRA, through its first few directives, has prohibited an entity from providing non-auditing services to an audit target during auditing. As studies have noted, it is essential that providing non-audit services to the ongoing audit target has produced lower-quality audits.[641] NFRA also prohibits an entity from providing auditing services if it has a history of a business relationship with the audit target. Such measures maintain the auditor's independence and remove the conflict of interest.

[639] Ahuja N., & Luniya V, Introduction To Environmental, Social, And Governance (ESG) Disclosures In India With An Overview Of The Global Standards On ESG, 14th November, 2022, Available at https://www.mondaq.com/india/diversity-equity--inclusion/1250572/introduction-to-environmental-social-and-governance-esg-disclosures-in-india-with-an-overview-of-the-global-standards-on-esg.

[640] Enron hired Arthur Anderson for accounting and auditing purposes. Arthur Anderson in fear of losing a potentially lucrative client overstated the profits of Enron resulting in a reckless practice. This resulted in US framing oversight legislation called the Sarbanes Oxley Act of 2002, which created a Public Company Oversight Board (PCAOB). For more, read Alex Berenson, "*Tweaking Numbers to Meet Goals Comes Back to Haunt Executives*", N.Y. TIMES, June 29, 2002.

[641] McCoy, P. A. (2002). Realigning Auditors' Incentives. *Conn. L. Rev.*, *35*, 989.

Auditor access is another important aspect of auditing as it depends upon the audit target to furnish documents, as they can claim trade secret rights or other Intellectual property rights. It is more accurate in the case of technologies as algorithms are unique to each system; thus, furnishing such information to unknown third parties is detrimental to a business providing the technology. In AI auditing, civil society organisations have been threatened and subpoenaed. Businesses have used non-legal strategies (like structuring the product in a way that does not allow test points, delayed communications, or unclear data documentation) to interrupt audit practices.[642] The legislation or through an executive order, NFRA can release a list of accredited and certified auditors to access any technology system's 'black box'. Such certification should not be limited to only the top four auditing firms but extend to lawyers, civil society organisations, academic researchers, and public interest groups. The entities in the list should have complete access to auditing technologies to be deployed in schools; however, for harmonisation purposes, they meet a common benchmark of professional standards that NFRA can again draft.

The tool of auditing, if performed independently and given full access, holds potential to uncover the 'messy context' in which the technologies are being designed, developed, and deployed. DPIAs can be audited to hold the stakeholders to account, i.e., a) By noting the reasons why a particular data was collected and how was it measured, b) listing the data collectors and cleaners, c) Reasons behind choosing a particular database, and d) By monitoring data drifts occurring post-deployment. Capturing such incentives and motivations during auditing can help holding the relevant stakeholders to account.

2.3. Transparency

Like fairness, transparency is also an accountability mechanism for algorithmic systems. The principle of transparency advocates for looking inside a technological system and revealing its facts or the absolute knowledge of how it works. Transparency has an epistemological assumption that more information means more facts are revealed, which leads to the ultimate

[642] Levine A., Chilling': Facial recognition firm Clearview AI hits watchdog groups with subpoenas, Politico, 24th September 2021, Available at, https://www.politico.com/news/2021/09/24/clearview-ai-subpoena-watchdog-groups-514273; Brandom R., Facebook shut down German research on an Instagram algorithm, researchers say, August 13, 2021, Available at, https://www.theverge.com/2021/8/13/22623354/facebook-instagram-algorithm-watch-research-legal-threat, Persily, N.,'Facebook hides data showing it harms users. Outside scholars need access', October 5, 2021, Available at https://www.washingtonpost.com/outlook/2021/10/05/facebook-research-data-haugen-congress-regulation/.

truth.[643] The logic behind more availability of facts/truth is to allow the observers to judge whether the system is working as intended. Transparency is considered a precondition for a harmonious society in which a system's '*true essence*' is uncovered.[644] The transparency tool has been used to apply control and surveillance over black, mixed-race, and indigenous populations, to identify their '*wrongdoings*' and accordingly apply '***censure'***.[645] The transparency tool has been used to apply control and surveillance over black, mixed-race, and indigenous populations, to identify their '*wrongdoings*' and accordingly apply '***censure'***. Thus, transparency is not only about revealing the truth but also controlling and addressing the risks emanating from the said truth. However, herein transparency presumes that every uncovering is explainable and interpretable and that consumers/users would be able to understand the nuances of a given system. The promises of transparency and openness can be found in Freedom of Information laws, product safety, consumer, fiscal reporting, and environmental laws. As noted in other legal and policy areas, transparency leads to organisations' answerability by compelling them to provide documentation, thereby demanding accountability. Thus, transparency is a means to achieve accountability, not a form of accountability itself.

In the context of emerging technologies, algorithmic transparency has earned its merit by way of several studies and books.[646] The literature does not limit the concept of algorithmic transparency to algorithms but embeds it in each stage of the lifecycle, i.e., Design, Development and Deployment. It is not a novel concept, as computer scientists have been deploying diverse approaches to explain computers' inner functioning and algorithms to computer science students. Transparency has been seen as an ideal tool in computer science as it allows '*knowing*' by

[643] Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *new media & society*, *20*(3), 973-989.
[644] Christensen, L. T., & Cheney, G. (2015). Peering into transparency: Challenging ideals, proxies, and organisational practices. *Communication theory*, *25*(1), 70-90.
[645] Browne, S. (2015). *Dark matters: On the surveillance of blackness*. Duke University Press. Browne explains how there were architectures of surveillance and control in the 18th century New York called as '*Lantern Laws*', where marginalised sections of the population could not walk escorted by a white person. The white person was responsible for uncovering the wrongdoings and censuring.
[646] Pasquale F (2015) The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge, MA: Harvard University Press; Diakopoulos, N. (2016). Accountability in an algorithmic decision making. *Communications of the ACM*, *59*(2), 56-62; Brill, J. (2015). Scalable approaches to transparency and accountability in decision making algorithms: remarks at the NYU conference on algorithms and accountability. *Federal Trade Commission*, *28*; Zara, C. (2015). FTC chief technologist Ashkan Soltani on algorithmic transparency and the fight against biased bots. *International Business Times*, *9*.

'*seeing*' the computational technology.[647] However, transparency is limited in many ways, which need to be understood to better appreciate the Right to explainability and interpretability, the two rights in the GDPR that support stronger transparency requirements. Annany and Crawford highlight ten limitations of the transparency ideal but caution that it is not an inclusive list but rather '*entrenched shortcomings*'.[648] The following ten limitations risk not only the inclusion of the said rights in the GDPR but also make the transparency regulations for emerging technologies an inadequate idea: a) Increased visibility due to transparency undoubtedly reveals corruption and power asymmetries within a system, but it also exposes people who are responsible which in many cases might hide and become impossible to trace in future, b) Increased transparency overlooks the questions of why something is revealed which might lead to leakage of sensitive personal information available for public scrutiny and misuse. Unnecessary information might make its way out in the public leading to bad actors gaming the system,[649] c) Organisations might reveal too much information by way of meeting their transparency requirements that the central information remains hidden and the receivers are distracted, called as strategic opacity,[650] d) Transparency can lead to information senders deciding what amount of information should be disclosed leading to incomplete openness, in absence of specific standards on transparency,[651] Transparency presumes and puts burden on the individuals to seek more information, understand and interpret them, and understand its significance,[652] Transparency ensures revealing the truth however does not compel the organisations to publish it in a standardised, clear and accurate way.[653] g) Depending upon specific areas, professionals have exercised transparency based on who should have access and who should hold people accountable and resolve risks[654], h) Transparency does not always lead to understandability, and therefore it is restrictive to the '*seeing*' and '*knowing*' aspect rather than appreciating the dynamic interaction within various

[647] Datta, A., Tschantz, M. C., & Datta, A. (2014). Automated experiments on ad privacy settings: A tale of opacity, choice, and discrimination. *arXiv preprint arXiv:1408.6491*.
[648] Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *new media & society*, *20*(3), 973-989., p. 978.
[649] Crain, M. (2018). The limits of transparency: Data brokers and commodification. *new media & society*, *20*(1), 88-104.
[650] Stohl, C., Stohl, M., & Leonardi, P. M. (2016). Digital age| managing opacity: Information visibility and the paradox of transparency in the digital age. *International Journal of Communication*, *10*, 15.
[651] Fox, J. (2007). The uncertain relationship between transparency and accountability. *Development in practice*, *17*(4-5), 663-671.
[652] Schudson, M. (2015). *The rise of the right to know: Politics and the culture of transparency, 1945–1975*. Harvard University Press.
[653] Schnackenberg, A. K., & Tomlinson, E. C. (2016). Organizational transparency: A new perspective on managing trust in organization-stakeholder relationships. *Journal of management*, *42*(7), 1784-1810.
[654] Abbott, A. (2014). *The system of professions: An essay on the division of expert labor*. University of Chicago press.

constituents of a system. It emphasises that '*what one knows*' is less important than '*how one knows*',[655] i) Transparency might not be technically possible due to the fast and automated nature of technologies like facial recognition in which data controllers might themselves not have knowledge or access to the errors surfacing,[656] and j) Computational systems change over some time, more so in case of emerging technologies. Technologies like facial recognition, emotion recognition, or AI tools to predict drop-out rates require continuous data supply. Thus, supplying information about the training and testing dataset at a particular time interval will only give transparency for the time being. A technology like Aadhaar that is embedded with multiple technologies and operates in various environments is technically not feasible to see inside a '*single*' system and determine the transparency of the entire complex environment.[657]

Transparency also forms part of child development studies that explain to students the constituents and patterns of a given theory. For instance, the kindergarten learning method teaches young children the patterns of a given object and how each constituent within a pattern interacts.[658] It enables a child to understand the complete construction of an object. Dewey has applied a similar theory in the experiential form of learning where a programming language is taught to children by simulating the computational model in their environment so that a child understands the model's design materiality, context, and complexities.[659] Such theories and abovesaid limitations of transparency point out the dangers inherent in applying the tool in complex technology environments, especially when children are at stake. However, the thesis does not agree with Ananny and Crawford's claim of transparency that it cannot explain and govern the human and non-human actors who operate such technology. The thesis now looks at the two rights enshrined in the GDPR in an attempt to claim that data controllers can be obliged to be transparent effectively if current regulations are amended and contextualised, thus hoping to counter the above claim automatically. It is also important to note here that the rights under GDPR are not mentioned under the present Indian DPB, nor do any other transparency requirements on the data fiduciary.

[655] Resnick, M., Berg, R., & Eisenberg, M. (2000). Beyond black boxes: Bringing transparency and aesthetics back to scientific investigation. *The Journal of the Learning Sciences*, *9*(1), 7-30.
[656] Diakopoulos 2016, Supra note 594.
[657] Krawford, supra note 596.
[658] Stiny, G. (1980). Kindergarten grammars: designing with Froebel's building gifts. *Environment and Planning B: Planning and Design*, *7*(4), 409-462.
[659] Dewey, J. (1986, September). Experience and education. In *The educational forum* (Vol. 50, No. 3, pp. 241-252). Taylor & Francis Group.

2.3.1. Right to Explainability and Interpretability

There has been a longstanding issue in privacy law that algorithmic harms arise from how technology stigamatise a class of individuals. However, the privacy law remedies, or the regulations suggested in a data protection law are often considered from an individualistic perspective. It is to be noted herein that the Right to explanation and Interpretability flows from GDPR, as it will be showcased below, as an individual data subject right. An individual must learn how a particular technology work, adapts, and then discuss, deliberate, and modify the technologies they use or are subjected to. Computer scientist Edward Felten and Professor Pamela Samuelson define such process as' *freedom to tinker*'.[660] Professor Samuelson adds that such freedom to inquire and study a system can lead to autonomy, dignity, and human flourishing, which are essential to the Right to privacy.

Another thing to note is the overlapping features between DPIAs and the Right to an explanation as the conclusion to both is a better understanding of the technology from the '*inside*'. Nevertheless, while DPIAs is an obligation on the controller to furnish the records of how their technology works and why it is necessary to deploy a given technology, seeking an explanation in an interpretable way is a right of data subjects to seek a specific answer related to them. This thesis claims to let them co-exist so that if DPIAs miss out on revealing certain vital truths, a data subject can push the data controller to open the black box and demand further scrutiny. Further, the Right to Explanation also suffers from legal and enforcement questions. While the legal question is whether the Right to Explanation even exists under the GDPR framework, the enforcement question seeks to challenge its implementation as a right. While engaging with both questions, the thesis will prove that Right to Explanation as a right is essential, especially for children, which will bring more transparency needed for an effective grievance redressal system.

The current Indian DPB does not explicitly mention the Right to Explanation, but Section 12 provides data subjects with the Right to Information on personal data. Upon further reading Section 12, data subjects can seek a limited information set from a controller. First, the Right to information has the Right to confirmation subsumed under it, allowing the subjects to confirm if their data is currently under processing or has been processed. Second, it allows seeking the list and amount of their data getting processed, along with the identities of data controllers with whom it is being shared. Section 12 also contains a broad statement, '*any other information as may be*

[660] Edward Felten, "*Freedom to Tinker: The Struggle to Access Devices You Own"*, Princeton University; and Samuelson, P. (2016). Freedom to tinker. *Theoretical Inquiries in Law*, *17*(2), 562-600.

prescribed,' but the word '*information*' in this context finds mentioned in only Section 6. Section 6, regarding information given to a data subject, is a replica of information that can be sought under Section 12. Thus, both the provisions, even if read together, provide a narrow information set to the data subject. Such information is insufficient for data subjects to challenge the authenticity of the decisions made by technology, verify the information given by the controller, and seek redress in case of grievances. Thus, it is essential to compare the Rights under the Indian DPB with the GDPR to learn some lessons.

Similar to the Indian DPB, the GDPR also does not have an explicit Right to Explanation in its text. However, upon reading Article 22 and Article 15 of the GDPR and the relevant recitals, the Right to explanation seems meaningful. Article 22(1) provides the Right to the "*data subject not to be subject to a decision based solely on automated processing, including profiling which produces any legal effects or significantly affects him or her*". It does not prima facie provides any right of information, let alone explanation and Interpretability. Upon further reading, Article 22(3) obliges the "*data controller to implement suitable measures to safeguard data subjects' rights and freedoms in case of automated processing used, at least the right to obtain human intervention that provides an avenue for the data subject to express its point of view and to contest the decision*". Two things to note from Article 22(3) are that it applies only in cases of automated processing where the data controller has to implement some measures, and a specific measure has been provided by way of using at *least*,' i.e. a minimum implementable measure in the form of '*human in the loop*' to allow the data subject to seek grievance redressal. Upon reading the two clauses of Article 22 together, it is clear that it provides a legislative vehicle to include specific '*suitable measures*', but the Right to explanation is still explicitly absent. A recital attached to Article 22 defines *automated processing* as a measure where personal aspects of an individual are profiled, such as e-recruiting, credit scoring, etc. Recital 71(5) further states that such processing should be subject to suitable safeguards.[661] It provides certain '*should*' measures to be implemented by a data controller, and this is where the Right to explanation originates from within the GDPR framework. Recital 71(6) also states that such processing, like profiling, should not happen for a child, effectively prohibiting it. Having identified the roots of the said Right, recitals have been stated to be of persuasive value and do not create a substantial legal right.[662] Scholars have also specifically pointed out political reasons for intentionally including the Right to

[661] UK GDPR, Recital 71, Available at, https://gdpr-info.eu/recitals/no-71/.
[662] Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. *Duke L. & Tech. Rev.*, *16*, 18.

explanation in the recitals section.[663] However, none can state that the Right is absent in the GDPR framework because specific practical challenges have been intentionally omitted—this call not to remove the said Right demands strengthening its enforceability.

Another Article in the GDPR that is broader than Article 22 in providing features of a similar right to explanation is Article 15.[664] Article 15 joins hands with the abovementioned Section 12 of the Indian DPB, providing the data subjects the Right to confirm whether their data is being processed and access specific details. However, Article 15(1)(h) goes beyond its Indian counterpart, from which the Indian DPB could learn lessons. Article 15(1)(h) includes - *at least* in the context of automated decision-making - "*access to meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject*". By using the underlined phrases, Article 15(1)(h) opens up the possibility of opening the technology and understanding its entirety and its functionalities in the sense of how it operates, processes, stakeholders involved, targeting patterns, and the manner of deduction of outcomes. The scholars have also made a valid point of creating a difference between Article 15 subject access rights and Articles 13 & 14 that pertain to 'information rights'. While under Articles 13 & 14, there is an obligation on the data controller to provide information to the data subject at the time when personal data are obtained (implying ex-ante obligation before the data is fed into the system), under Article 15, the data subject can obtain data ex-post, i.e. once the data is under processing or has been processed. Reading all articles together brings further clarity: Although the Right to explanation is not present in the GDPR text, Recital 71 and Articles 13-15 allow the data subject to seek information along the entire system lifecycle. Accordingly, the Indian DPB should enact amendments to create a differentiation between sole and semi-automated processing - by banning the former in the case of children -and then expand the Right of information/access/explanation under section 12.

Since it is now clear that such a right exists, there needs to be a discussion on its practical implementation, further strengthening the argument in favour of its inclusion in the data protection law. The computer science community has regarded the Right to an explanation as a fundamental right responsible for creating incomprehensible black-box technologies for individuals subjected

[663] Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, *7*(2), 76-99.
[664] UK GDPR, Article 15, Available at, https://gdpr-info.eu/art-15-gdpr/.

to them.[665] Edwards and Veale state that two kinds of explanations are possible in the data protection and privacy context: Model Centric Explanations (MCEs) and Subject-Centric Explanations (SCEs). While MCEs provide a set of information applicable to a group - like how a technology is trained and built, how data is collected, and technology's predictive skills - SCEs are more individual specific and personalised explanations - like which specific data records used, what changes in the input data of an individual would change the outcome, are individuals similar to the data subject erroneously classified before etc. Thus, unlike MCEs, SCEs build a personal relationship between the data subject and its data, providing a much more 'meaningful explanation'. Most of the questions forming part of the above table for DPIAs are more model-centric than subject-specific. It also indicates the difference between the purpose of DPIAs and the Right to Explanation. While DPIAs are a tool to make the design, development, and deployment of a technology fairer, the Right to explanation allows the data subject to indirectly make technology transparent by seeking individualised questions not covered by the DPIAs.

The thesis appreciates that providing meaningful explanations is only sometimes technically feasible and acts as an undue burden for data controllers. It is because at the data processing stage, AI/ML applications process data beyond the control of a data controller and, in some cases, the third-party software developer or a data scientist, as shown in the previous chapter. Like some collected inputs need more precise or more convenient human interpretation, similar processing or post-processing predictions might be challenging to spell meaningfully. For instance, in the case of an emotion recognition tool, input data can be variables that are difficult to quantify - like how long a child takes to click on a laptop, time spent by a child reading and the expression therein, or a text written by a child but then deleted without posting - these variables certainly provide information about individual characteristics. However, they are highly context-based and thus beyond any specific interpretation. It is a fact that explanations, especially in the case of technologies targeting children, should be clear, concise, legible, and transparent. Thus, for at least such technologies, we must ask - Can we comprehend the complexities of a school? Do we need technology for taking decisions on highly context-based data? If yes, can we explain it to a child, let alone its guardians? If not, such technologies should be prohibited at the design stage. If certain technologies, by their inherent technical functionalities, are devoid of explanation, they should be called upon to breach a right granted to a data subject and therefore be banned.

[665] Tickle, A. B., Andrews, R., Golea, M., & Diederich, J. (1998). The truth will come to light: Directions and challenges in extracting the knowledge embedded within trained artificial neural networks. *IEEE Transactions on Neural Networks*, *9*(6), 1057-1068.

Thus, Right to Explanation in an interpretable manner is key to make the entire system of design, development and deployment transparent. Documentation of key questions relevant for privacy aids fairness, inspection of the documentation leads to accountability, and the right of the data subject to seek explanation makes the entire process transparent. Each principle is interdependent on the other that provides increased visibility to the three-part process. For instance, seeking explanation on what information of a data subject is being collected, how its processed, why a less explainable algorithm is chosen for processing, push the teams to think around model selection, model training and testing. Such technical bits need to be made available to data subjects in an accessible and legible user interface (legally by product teams) for them to understand the 'surveillant assemblage' in making.[666]

2.4. Equity

2.4.1. Optimising Consent in the AI/ML Age

Both the Indian DPB and the UK GDPR framework defines consent identically as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by a statement or by a clear affirmative action, signifies agreement to the processing of personal data*".[667] There is a minor difference between the two, wherein the Indian DPB at the end adds. *Agreement to processing personal data 'for a specified purpose',* which in the UK GDPR is absent. Thus, the Indian DPB is much more specific and unambiguous concerning the type of processing allowed. It connects it to the purpose specified by the data fiduciary in the notice sent to the subject. It limits the scope of the consent to what is written in the notice, thus also curtailing 'function creep'.

The previous chapter talks in detail about the connection between notice in consent in greater detail but also highlights the limitation of the two concepts regarding children. Consent can be considered equitable when it recognises its limitations and acknowledges the contexts in which a data subject provides it. Children of different age groups, under different kinds of parental and societal pressures, can be tamed easily to agree/disagree, which raises questions on the validity

[666] Infra Part C. Globally, under consumer protection regimes, product liability places an impetus on manufacturers/product teams to provide sufficient information in legible manner.
[667] Section 7 of the Indian DPB and Article 4(11) of UK GDPR.

and authenticity of the parental consent itself.[668] Apart from the parental consent, the age of maturity at which a data subject should start giving consent, ways of obtaining, managing, and storing consent, and whether consent should be differently obtained should depend on the risks posed by a given technology are other legally contentious issues, which if left unanswered would increase children's privacy risks.

UK GDPR framework and scholarly user design research have potential principles that could help regulate how consent is obtained, recorded, and managed. Article 7(2) and Recital 42 of the UK GDPR provide specific consent guidelines. They call for clear and straightforward language that avoids legal or technical jargon. It also asks to avoid using vague, ambiguous words or expressions and to keep the consent request concise and specific. The present Indian DPB has adopted similar phrases in line with the recommendation of the Srikrishna committee report in the form of five principles.[669] The five principles to design a privacy policy document (including consent and notice forms) include a) *Approachability* (to minimise the intimidating nature of the document), b) *Comprehensibility* (Simplifying the content to make it widely understandable), c) *Helpfulness* (The text assists the engagement and is not a passive vehicle, for instance, intra and interlinking of a document, or using colour codes, icons, and other non-textual designs to aid meaning of the document), d) *Legibility and Readability* (Optimising the page layout and typography to make it effortless to read) and e) *Conscientiousness* (Giving users the control over what they give consent, like ensuring there are no pre-checked boxes, or consent should be unbundled, i.e. separate consent for each purpose, etc.). Such principles, whether applicable for parental consent or directly from children, should form part of the main text of the Indian DPB, especially when it does not include any recitals. Including such user Design principles would contextualise the notion of consent. Further, Section 7(3) of the Indian DPB asks the data controller to seek consent in languages known to the data subject - the languages mentioned in the Eight Schedule of the Indian Constitution - making it an equitable provision.

Though the Indian DPB weaves equity into the legislation concerning seeking consent, it should explicitly include the five principles of the Srikrishna Report. However, because of the changing technological landscape, the idea of seeking consent might also change or be burdensome for

[668] Taylor, M. J., Dove, E. S., Laurie, G., & Townend, D. (2018). When can the child speak for herself? The limits of parental consent in data protection law for health research. *Medical law review*, *26*(3), 369-391.
[669] Justice Srikrishna Committee Report, Supra note 457.

the data subjects. For instance, though unbundling consent and taking consent at all process stages has the potential, it can also amount to consent fatigue. Though the Srikrishna Committee report principles help strengthen certain principles of consent like its reversibility, informed, and specificity, the idea of '*freely giving*' consent in cases of children still stands weak. It is due to the inherent power dynamics involved in a school setting (as explored in the third and fourth chapters), and legally it is the parent/guardian given the responsibility to provide consent on behalf of children, thus raising questions on consent '*free*' nature. The following sub-section discusses the limits of parental consent and explores the conditions and circumstances in which children can be directly approached for consent purposes.

2.4.2. Limits of Parental Consent and the Call for Assent

Consent should be an age-appropriate concept considering evolving capacities. Also, while children are not allowed to provide consent under the law until the age of majority, their assent should be documented alongside parents' consent for CPO to consider. CPOs can again be used to formulate questions for seeking children's assent, depending on children's ages and abilities. Such questions must be clear, concise, and legible to ensure their accessibility and the ability of children to understand. A study shows that the unclarity in questions is directly proportional to the decline in response quality, which can defeat the entire purpose of the assent.[670] For younger children, seeking assent should be an interactive exercise rather than a set of terms and conditions. It is also best to use general language rather than technical jargon to introduce technical concepts related to technology and seek approval. Teachers and school administrators should use images, pictures, films, and visual representations of technical concepts or cartoons to seek children's approval.

Even after utilising such visual design techniques - that are beneficial for children and their parents giving consent on their behalf - the idea of parents providing consent until the child attains 18 discredits children's growing capacities and maturity levels. While Indian law determines the age of the children through their chronological age, in the UK, it is determined by *Gillick Test*, a test borrowed from health research. The test determines whether the minor has the capacity if and when the child achieves sufficient understanding and intelligence to understand what is proposed

[670] Fuchs, M. (2008). The reliability of children's survey responses: The impact of cognitive functioning on respondent behavior. In *Proceedings of Statistics Canada Symposium* (Vol. 11, pp. 522-530).

fully.[671] According to health guidance, for a minor who has positively passed the Gillick test, consent can be overridden in certain cases.[672] For instance, such a minor's consent would not be admissible if the decision is against the public interest or necessary to protect the child from the risk of death, abuse, addictions, or self-harm. Such overriding abilities have been criticised in scholarly research as not child-focused but protective of doctors.[673] Further, the Gillick test is also criticised as it places an onus on the child to prove their competence; instead, according to Alderson and Montogomery, the onus should be on parents/guardians to prove that their child is not capable enough.[674] While they clarify not to be against parental consent but suggest that it should not be against the child's wishes. Essentially, they are advocating for a tripartite child-centric model where the data controller, parents, and child have continuous conversations to build trust and cooperation, ultimately yielding free and voluntary consent. Such a tripartite relationship has been lauded within the health research community, which states. At the same time, the Gillick test can be continued to determine the children's capacity to seek consent; those who fail the test should be part of the '*assent process*'. In health research, the assent process is participatory. It involves and explains to children the nature of the surgery, the tests that would be conducted, their impact and consequences, and factors that should be considered while giving consent. Herein, the child can provide assent to the doctor, upon which the doctor seeks parental consent. The assent process minimises the risks of parents trampling on the '*best interests*' of the child.[675]

While the assent process is participatory and child-focused, it is flexible. The assent process is limited in terms of a) the Conceptualisation of its definition and how it is different from consent, b) Obtaining assent through assent forms (similar to consent forms) that might challenge a child's reading abilities and comprehension powers, c) Uncertainty of the age-group from which to seek

[671] *Gillick v West Norfolk and Wisbech Area Health Authority*. 1985. 3 All ER 402, HL, at 422, per Lord Scarman.
[672] General Medical Council. 0–18 years, Guidance for All Doctors. London: GMC 2007, s.46.
[673] de Zulueta, P. (2010). Choosing for and with children: consent, assent and working with children in the primary care setting. *London Journal of Primary Care*, *3*(1), 12-18.
[674] Alderson, P., & Montgomery, J. (1996). *Health care choices: making decisions with children* (Vol. 2). Institute for Public Policy Research.
[675] Best interests are the bedrock principle for the protection of child rights as mentioned in the UNCRC. Kopleman identifies three stands of the usage of best interests. First, the principle can be used as a threshold for intervening in parental consent if it endangers the child. Second, best interest is like 'a lighthouse in the sea' paving and steering a child's welfare toward a gold standard, and third, best interest principle is for reasonableness i.e. choosing the best alternative that a reasonable person would have chosen in a given circumstance. For more details, read Kopelman, L. M. (1997). The best-interests standard as threshold, ideal, and standard of reasonableness. *The Journal of Medicine and Philosophy*, *22*(3), 271-289.

assent,[676] and d) When will parental consent supersede child's dissent, for which the word dissent needs to be fleshed out as it is definition is absent from the current health guidelines.[677] On the conceptualisation point, it would be fair to impose similar principles of consent to assent. In effect, both treat the subject as a consumer of a particular product or service. A child-producing assent should also be benchmarked against similar principles of free, informed, specific, and capacity to be withdrawn. However, the assent process empowers the fifth principle of consent - absent in explicit terms from the GDPR and the Indian DPB - participatory. On the uncertainty of age groups, the WHO Ethics Review Committee provides an effective by stating, "while the age at which this informed assent should be taken varies, one should consider asking for assent from children from seven years of age". While it is uncertain why WHO has taken the age of seven, the present thesis advocates for applying the assent process to all groups of children yet not mature enough, based on the Gillick test.

The final two points of contestation, i.e., Obtaining assent through forms and conflict between parental consent and children's assent, demands further analysis, as contextual factors of low-income, conservative societies, illiteracy, complex family relationships, infrastructural constraints regarding documentation, and vague regulations defeat the efficiency of assent.[678] Such factors are also applicable to weakening consent in such settings. While obtaining assent through forms or consent from parents requires a design-based framework (discussed in the following sub-section), this sub-section would complete its analysis by avoiding the above-stated conflict.

Firstly, in the context of technology deployed among low-income or illiterate societies, children may have more chances of getting an education than their parents. Also, children might be more exposed to technology concerning parents, enabling them to read, write and better equip themselves with the risks and dangers of deploying a given technology.[679] Secondly, a child might come from a society where it is taught not to speak before elders, exhibiting more parental control than the child's best interests. In patriarchal societies like India, it is not uncommon for elders to

[676] Royal College of Pediatrics, Child Health: Ethics Advisory Committee: Guidelines for the ethical conduct of medical research involving children. Arch Dis Child 2000, 82:177–182. The age of assent differs in the WHO report, World Health Organisation Research Ethics Committee: The process of obtaining informed consent, Available at http://www.who.int/rpc/research_ethics/ Process_seeking_IF_printing.pdf.
[677] Cheah, P. Y., & Parker, M. (2014). Consent and assent in pediatric research in low-income settings. *BMC Medical Ethics*, *15*, 1-10.
[678] Ibid, p. 4-6.
[679] Molyneux, C. S., Peshu, N., & Marsh, K. (2004). Understanding of informed consent in a low-income setting: three case studies from the Kenyan Coast. *Social science & medicine*, *59*(12), 2547-2559.

decide on behalf of the entire family. Thirdly, due to complex family relationships, parents and children are not on talking terms, or adopted children might not be considered valuable for guardians, where taking parental consent would be diminishing. Fourthly, having information sheets or assent forms applies to societies with suitable infrastructure to maintain, review and update such paperwork. In all such situations, seeking the child's assent/dissent holds much importance and should supersede parental consent/dissent.[680] The above circumstances are an exhaustive list and consider certain contextual factors, but the thesis appreciates that this is an area of further research beyond legal research. Health research provides us with the assent process that can be borrowed into the data protection laws as a precursor to parental consent and safeguarding the child's best interests. We now move on to the final discussion on the consent that utilises the research from the user-design community to further empower children's participation in the consent process.

2.4.3. Involvement of Children & Grievance Redressal Framework

The appropriate measures designed by a data controller should involve children's views before operation. Children are both rightsholders and stakeholders in case any business products or services are targeted at children, directly or indirectly. It is important to understand children's views to capture their context for a given technology, which otherwise would lead to discrimination. For example., facial recognition technologies deployed in a classroom might not be able to predict the reason behind a child's gloomy face because it can be due to low-income household impact, a bad morning breakfast, or the effect of parents' work. Evidence shows that parents are often unaware of their children's technological usage and the rights they should ideally possess in a technological environment.[681] Without proper engagement with each child, in the absence of other seniors, capturing such myriad sets of information is potentially impossible. UNICEF in its report on "*Engaging Stakeholders on Children Rights - A tool for companies*", specifies certain circumstances when a child should be consulted directly: a) When children can provide information that cannot be accessed through other child rights stakeholders, b) When children's direct voices will provide information to the input of other stakeholders, and, c) When

[680] Rajaraman, D., Jesuraj, N., Geiter, L., Bennett, S., Grewal, H., & Vaz, M. (2011). How participatory is parental consent in low-literacy rural settings in low-income countries? Lessons learned from a community-based study of infants in South India. *BMC Medical Ethics*, *12*(1), 1-9.
[681] UNICEF Innocenti Research Centre, Child Safety Online: Global challenges and strategies, United Nations Children's Fund, Florence, Italy, May 2012, p. 7, www.unicef.org/pacificislands/ict_eng.pdf.

adults comments need to be validated.[682] While point b can include input on how children experience or use a product or service, point c can validate whether parents' consent adequately reflects the child's position, both applicable to the present thesis context. While in some cases, businesses would include child rights advocates, parents/guardians, teachers, or other school administration in the stakeholder consultation process, as it will be shown below through a six-stage framework, direct involvement of children of all age groups is preferred and can be done by taking creative approaches. While the identified stakeholders can facilitate the engagement process, focus group discussions should directly involve children.

Even if engaging a child at each level is impossible, a core set of agreed legal norms can be borrowed from international human rights standards. United Nations Convention on the Rights of the Child (UNCRC) and the Universal Declaration of Human Rights (UDHR) offer the most promising set of ethical standards that a data controller can use for emerging technologies. The reason for choosing UNCRC and UDHR as legal norms is their specificity towards encompassing children. However, also they are widely recognised as essential in a constitutional democracy. Also, said instruments were adopted during World War II as a commitment to human rights, democracy, and law. If any technology intentionally or discreetly excludes individuals from accessing their rights, services, resources, opportunities, and entitlements, they could seek fairness under the said instruments.

While no specific reasoning is provided under the Indian DPB for including children as a particular category, Recital 38 of the UK GDPR states, "*Children require specific protection concerning their data as they may be less aware of the risks, consequences, and safeguards concerned and their rights.*" A similar argument is reiterated in Article 3 of the UNCRC, which states: "*In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration*". Specifically inviting views of the children when technology is designed for them or their data is processed, would be compatible with Article 12 of the UNCRC where it states that "*Every child has the right to express their views, feelings, and wishes in all matters affecting them, and to have their views considered and taken seriously*". Further, Principle 18 of the United Nations Guiding Principles on Business and Human Rights calls on companies to "involve

[682] UNICEF, Engaging stakeholders on children's rights, '*A tool for companies unite for children'* First edition, Available at, https://sites.unicef.org/csr/css/Stakeholder_Engagement_on_Childrens_Rights_021014.pdf.

meaningful consultation with potentially affected groups and other relevant stakeholders".[683] The future Indian data protection regulator can refer to the principles and guidelines made by the children in Scotland for their effective participation and engagement.[684] While the guidelines are not focused on how technology interacts with children, they can be applied in any context. The thesis now adapts the six fundamental principles and guidelines in the Indian school context where technologies are being deployed to assist the future regulator in building upon it and satisfying the requirements of UNCRC and UDHR by inclusion in the current data protection framework.

The *first stage* of Planning and Coordination focuses on the participation and engagement of children from the design stage itself. While it should be technology-specific engagement, organisations or school administration targeting children should ensure consent is taken at each stage of the project, meaning while deciding to bring technology, while furnishing tender, or when the third party maintains the said technology changes. Such consent should be taken from all age groups of children as the sensitivity of the privacy right would differ in particular age groups (discussed more in detail in the following sub-section). For such purposes, a student union can comprise students of all age groups, independent of their guardians/parents. In smaller schools, it can be the class monitor of each grade, documenting the concerns of each child and representing them at the planning stage. Such planning and engagement should only be done during certain times of the year, like exam periods; otherwise, it would induce unnecessary burdens and defeat the purpose of meaningful redress. Before the engagement starts, school administration should supply a DPIA of a particular technology for the children to make informed decisions (necessary for privacy) and seek their Right to explanation if they deem fit. It should be an obligation as part of the data protection framework for the school administration to publicise these records for audit and fairness purposes, which ensures the Right to privacy of all children has been taken into consideration.

The *second* stage of inclusion demands involving the participation of vulnerable and marginalised sections of children, especially children with disabilities, ensuring representation of all genders,

[683] Office of the High Commissioner for Human Rights, '*Guiding Principles on Business and Human Rights: Implementing the United Nations',* Protect, Respect and Remedy Framework, United Nations, New York and Geneva, 2011, Available at www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

[684] Children in Scotland, '*The participation and engagement of children and young people: Our principles and guidelines*', Available at, https://childreninscotland.org.uk/wp-content/uploads/2017/11/Principles-and-Guidelines-FINAL.pdf.

castes, and religions and removing barriers in their participation. It is also essential to ensure that at each stage of the process, feedback is taken through an accessible form. For instance, school administrations should acknowledge the religious festivals or specific religions from which children might not want to be regularly monitored. Children, parents, and child rights bodies should be consulted before installing cameras, emotion recognition tools, or facial recognition systems. Further, similar steps, as discussed in the first stage, should be implemented to make the process fair and equitable.

The *third* stage of child protection calls for awareness of child rights and providing child protection training to those responsible for handling children's data. It would be highly possible that even the principal of a school or senior teachers might not know how to handle children's data. Therefore, it is imperative for the school administration and the third party deploying the technology to undertake children's training, conduct a child rights impact assessment, publicise the result, and share it with children (student union) and parents before deploying a given technology. While privately run schools should appoint an on-call Designated Child Protection Officer (CPO), the government should appoint District-level CPOs to ensure responsible design, development, deployment, and usage of any given technology. Such CPOs could be supervised by a state Data Protection Regulator (DPO). The schools should be responsible for maintaining and updating CPOs' contact details in school diaries so that they are accessible to both parents and children. The role of the CPO should be defined in law, which can include determining the appropriate methodology for consulting children that should take the type of data involved, target demography, and build upon the local structures, practices, and customs into account.[685] Further, the CPO must safeguard the children participating in the engagement process and their identity. They might be under threat or pressure from parents, school administration, local politicians, police, or any other authoritative figure.[686] As one of the measures, no photographs, videos, or images should be

[685] European Union and United Nations Children's Fund, 'Module 3: Child Participation', EU-UNICEF Child Rights Toolkit: Integrating child rights in development cooperation, UNICEF Programme Division, New York, 2014. Available from: www.unicef.org/eu/crtoolkit/toolkit.html. Also read, Lobe, B., Livingstone, S., Olafsson, K., & Simões, J. A. (2008). *Best practice research guide: How to research children and online technologies in comparative perspective*. EU Kids Online, The London School of Economics and Political Science, Available at www.lse.ac.uk/media@lse/research/EUKidsOnline/BestPracticeGuide/FAQ/FAQsReport.pdf.

[686] European Union and United Nations Children's Fund, 'Module 3: Child participation', EU-UNICEF Child Rights Toolkit: Integrating child rights in development cooperation, UNICEF Programme Division, New York, 2014. Available from: www.unicef.org/eu/crtoolkit/toolkit.html.

allowed during the engagement process.[687] However, for transparency purposes, the minutes of the meetings should be recorded (that should form part of each quarterly DPIA), wherein names of the participating children should be redacted/anonymised.

The fourth and fifth stages discuss delivery and communication, respectively. Delivery pertains to creating appropriate space for children to come forward and share their views. It asks not to assume that children would understand the nuances and the context behind a particular measure. This is also relevant in the technology space, as especially younger children would not be able to understand the context of a given technology. Computer scientists and scholars in user design advocate for being creative when working with children. It is essential to take a creative approach, i.e. explaining the consequences of a given technology through visuals, cartoons, and immersive experiences than through one-sided lectures and slide presentations. Children can themselves be asked for their preferred method of communication.

The sixth and final stage is about seeking feedback and evaluating the decisions taken. While the Children in Scotland report does not refer to the technology context, it is essential to conduct evaluations and continuously seek feedback. The feedback stage might also reveal specific facts, based on the context, that the business was previously unaware of.[688] By their inherent nature, and technologies are prone to drifts, meaning they perform/predict differently in different circumstances. Such information should be passed to the children, and continuous evaluations using the abovementioned DPIAs should be conducted. While publicising a DPIA, the school administration must justify the reasons for conducting the said DPIA yearly and not quarterly. The results of the DPIA can be shown by using creative methods such as a blog or a short film, tying it to the previous stage.

[687] MediaWise and United Nations Children's Fund, The Media and Children's Rights, 2nd edition, MediaWise and UNICEF, January 2005. Available from: www.mediawise.org.uk/children/the-media-and-childrens-rights.

[688] Nomogaia, a non-profit organisation, consulted with children in school about the impact of uranium mining and energy operations in Malawi. While their other consultations with environment monitoring teams, community relations, and elders of the area revealed the deterioration of the environment, the children and the youth revealed fears that the presence of wealth due to companies' operations, would attracts criminal gangs, who hire children to siphon fuel from company trucks. This led Nomogaia to make efforts to stem criminal activity and monitor air quality. Thus, engagement with children might yield useful facets, that were not raised in previous engagements.

PART C - LOOKING AT OTHER INDIAN LAWS FOR REGULATION

3.1. Procurement Laws

Most systems procured by government schools or those that the government uses on children or teachers are either procured from a third-party provider or developed jointly through public-private partnerships. Due to the absence of central procurement law, such partnerships and procurement through them come to light only through transparency laws, like the Right to Information Act. In 2012, the government of India introduced a public procurement bill in the parliament upon being pushed by the United Nations Office on Drugs and Crime.[689] But with the government lapsing in 2014, it could not be debated and passed. In 2015-16, the present government stated in its budget speech, "*Malfeasance in public procurement can be contained by having a procurement law and an institutional structure consistent with the UNCITRAL Model*".[690] However, the present government has yet to introduce a Bill on the subject matter.

Technologies have the potential to pose a danger and undermine security, privacy, and other fundamental freedoms granted to an individual. Without proper oversight, transparency, and accountability of how the government has procured a particular system, there could be far-reaching consequences on the right to privacy of an individual. The absence of a central law in India only exacerbates the issue. The absence of a law means one cannot compel the government to be transparent about its public procurement practices. If the government has outsourced or purchased a system to a third-party technology developer, such outsourcing or purchase can remain hidden from public scrutiny. Whether it is intentional on the part of the government to not bring legislation to the parliament or not, such secrecy ironically contravenes the secrecy of an Indian citizen. Such secrecy also constrains the transparency requirements, like DPIAs, from being effective as no legislation mandates the government (when it is the data fiduciary) to include procurement information.

[689] The Public Procurement Bill, 2012, Ministry of Finance, Available at https://prsindia.org/billtrack/the-public-procurement-bill-2012; United Nations Office on Drugs and Crime, '*India: Probity in Public Procurement, Transparency, objectivity and competition in Public Private Partnership projects in line with the United Nations Convention against Corruption'*, Available at, https://www.unodc.org/documents/southasia/publications/research-studies/India-PPPs.pdf.
[690] Budget 2015-16, Speech of Arun Jaitley, Ministry of Finance, Feb 28, 2015, Available at https://www.indiabudget.gov.in/budget2015-2016/ub2015-16/bs/bs.pdf, p. 15, pp, 72.

As a policy interjection, the legislation is a panacea to which a government can resort. Policy issues like public procurement and principles like corruption, transparency, responsibility, security, and privacy are questioned. However, as research evidence shows, legislation is only sometimes a practical policy option to curb corruption in India.[691] Sometimes, the 'invisible infrastructure' is crucial for any policy interjection's success.[692] According to Kelkar and Shah, invisible infrastructure is the institutions, general laws, and accountability arrangements that are enough to take steps, reduce corruption and bring transparency in cases of public procurement.[693] It can be possibly true, as India has infrastructural machinery in place that manages public procurement processes. For instance, the Government E-marketplace (GEM) and the Central Procurement Portal (CPP) are two public platforms controlled by the central government. The government issues tenders through platforms/websites where bidders can apply for it and share their quotations. Rule 144 of the General Financial Rules, 2017 (which can be termed as a general transparency law in the invisible infrastructure) lays down guidelines that cover all public procurements conducted on GEM and CPP.[694] Rule 144 also has certain yardsticks that a central government procurement needs to abide by. Rule 144(2) & (3) is of particular importance as it obliges any public buyer to specify the quality of the product to be procured and technical specifications based on national technical regulations or, where relevant international standards.

There are similar state guidelines for procuring IT equipment in schools too. School/Education being a state subject under the Indian constitution, specific public procurement guidelines are framed only at the state level. For instance, Kerala has guidelines that require the vendor to show the teacher and IT coordinator how the technology works and obliges them to provide their contact

[691] Sukhtankar, S., & Vaishnav, M. (2015, July). Corruption in India: Bridging research evidence and policy options. In *India Policy Forum* (Vol. 11, No. 1, pp. 193-276). Delhi, India: National Council of Applied Economic Research.
[692] Roy, S., & Uday, D. (2020, August). Does India need a public procurement law? The Leap Blog, available at: https://blog.theleapjournal.org/2020/08/does-india-need-public-procurement-law.html#gsc.tab=0.
[693] Kelkar, V., & Shah, A. (2019). *In service of the republic: The art and science of economic policy*. Penguin Random House India Private Limited.
[694] Rule 144 states: Fundamental principles of public buying (for all procurements including procurement of works). Every authority delegated with the financial powers of procuring goods in the public interest shall have the responsibility and accountability to bring efficiency, economy, and transparency in matters relating to public procurement and for fair and equitable treatment of suppliers and promotion of competition in public procurement. For more details: https://www.panchayat.gov.in/documents/448457/0/General+Financial+Rules+2017.pdf/6dd9b934-4d97-3c27-5679-d2c026b7203f?t=1661411210166.

detail (both firm/personnel providing services).[695] The guidelines also place schools under a duty to display the list of equipment received, year-wise and source of funds. The guidelines also call for prior approval of the State Council of Education Research and Training and Kerala Infrastructure and Technology for Education (KITE) needed to deploy school IT equipment. A third-party auditor using yardsticks to document procurement processes can contribute to the FATE framework. The relevant auditor can also provide such knowledge to the CPOs and school administration and be a part of DPIA documentation. Thus, though there is no centralised legislation on procurement law, strengthening invisible infrastructure around it can be a way forward to empower individuals' data protection and privacy.

The global regulations around public procurement are also changing due to the advent of emerging technologies. The World Economic Forum (WEF) has presented some of the measures that can be adopted globally for public procurement that drive innovation in the market but also secures fundamental freedoms at an individual level.[696] The WEF AI government procurement guidelines address concerns about bias, transparency, privacy, and accountability. *First*, it asks the procuring organisation, including the government, to prepare a list of potential suppliers that abide by data protection laws, conduct DPIA, and have a data documentation process in place. Canada prepares a similar list of AI suppliers that use best practices like Explainable AI and meets global ethical standards.[697] *Second*, the guidelines mandate the AI supplier to submit details regarding the algorithm, like the datasets used, model training methods, whether humans can be in the loop, or its wholly automated decision-making algorithm. The government can take cognisance of the details sent, seek more information, and then accordingly hire a particular technology while recording the reasons for the same and making public the details sent by the third party. *Third*, the guidelines also suggest structures and mechanisms for the government to procure risks and impact of the technology procured and different measures that can be put in place to address those impacts. While WEF guidelines are not a silver bullet for improving the

[695] The Hindu, *Purchase of school IT equipment: rates revised in guidelines*, Feb 19, 2022, Available at https://web.archive.org/web/20220220063946/https://www.thehindu.com/news/national/kerala/purchase-of-school-it-equipment-rates-revised-in-guidelines/article65066399.ece.

[696] World Economic Forum, AI Procurement in a box: AI Government Procurement Guidelines, Toolkit June 2020, Available at https://www3.weforum.org/docs/WEF_AI_Procurement_in_a_Box_AI_Government_Procurement_Guidelines_2020.pdf.

[697] Canada Buys is a government website that lists tender opportunities and the organisations that win the tender round. To know winners of AI-related goods tender, refer to https://canadabuys.canada.ca/en/tender-opportunities?words=Artificial+Intelligence&record_per_page=50&current_tab=t&Search=Search&search_filter=&status%5B87%5D=87&status%5B1920%5D=1920.

public procurement process, they can serve as a template for the Indian government to harmonise its laws globally. Also, developing transparent guidelines around procurement can add to data quality, technology sourcing and assurance.

3.2. Information Technology Law

Generally, global data protection regulations call for using the best standards and practices to deploy technical and organisational measures to secure the technology. However, as technology progresses, new attack vectors and surfaces through which technology can be intruded are also discovered. Advanced intrusion tactics can also not be covered during auditing, as generally, auditors are from outside technical and security backgrounds. Without the proper discovery of security vulnerabilities, the technology would remain opaque and unfair, and data subjects would not be able to appreciate the consequences of the technology and seek grievance redressal, thus, risking children's privacy. The solution is creating a public vulnerability disclosure ecosystem where independent security researchers and benevolent hackers can reverse engineer the system and identify malicious vulnerabilities. Upon identification, the said ecosystem should be able to assess and then mitigate the risks and award those who aided such disclosure.

According to research by the Centre for Internet and Society, there seem to be four Indian Institutions that accept vulnerability reports from third parties.[698] The research states that besides the limited set of institutions allowing security reporting, several other challenges hinder the creation of an effective ecosystem. The study highlights three primary difficulties in the Indian context: a) There is an absence of a process through which someone can report a vulnerability to the government as their websites do not have contact information. Further, it is unclear as to whom to report among the four institutions; b) There is a lack of clarity as to what happens once a security vulnerability is reported, leading to numerous follow-ups by a researcher, leading to an additional barrier; c) There is no streamlining of forms in which a security vulnerability is reported, and sometimes it becomes an additional burden when the form has to be downloaded, filled and then posted by mail. Such forms also have pre-framed questions that limit a security researcher's responses. Also, in a country like India, the problems further exacerbate when such forms are

[698] The four entities are Indian Computer Emergency Response Team (CERT-IN), National Informatics Centre Computer Emergency Response Team (NIC-CERT), the National Critical Information Infrastructure Protection Centre (NCIIPC), and the Cyberdome initiative of the Kerala Police. Available at : https://cis-india.org/internet-governance/resources/Improving%20the%20Processes%20for%20Disclosing%20Security%20Vulnerabilities%20to%20Government%20Entities%20in%20India.pdf.

only available in English. Finally, d) The transmission of security vulnerabilities happens through insecure and unencrypted channels that might leak sensitive information due to intrusive methods used by malicious actors. Thus, there are procedural, communication, accessibility, and security challenges concerning independent and voluntary reporting of security vulnerabilities.

Unlawful disclosure of personal information violates several conceptions of privacy, including intimacy, secrecy, informational privacy, and personhood. As shown in Chapter 4, in the case of Aadhaar, school data stored in Aadhaar servers has been leaked multiple times. However, neither the government allowed third-party researchers to investigate the incident, nor has it taken steps to create an ecosystem of vulnerability reporting.[699] While the Indian DPB obliges the data fiduciary to take reasonable safeguards to prevent a data breach and notify the same, it does not allow a third party to report a breach or someone who could check such breach reporting. Even an audit, more so in cases of first or second-party audits, might not reveal the nature of the breach occurring in an organisation. To ensure the privacy of citizens, and especially of children, the government needs to create an environment that, rather than punishing activities that are needed for the discovery of vulnerabilities, motivates researchers to probe, scan, and access technologies, platforms, and related networks to make the entire ecosystem privacy-friendly and secure. A combined reading of Section 43,[700] Section 65,[701] and Section 66[702] of the Indian Information Technology Act, 2000 imposes penalties for damaging, tampering, or accessing any computer system, resource, or network. The main essence of the said sections is to impose penalties, fine or imprison any person who gains access to any computer system that has been classified as Critical Information Infrastructure (Aadhaar is included in it), or knowingly or intentionally penetrates or accesses a computer resource without authorisation of the person in charge or alters, deletes, conceals a computer source code. [703] The vagueness and ambiguity of the terms within the stated sections, like computer source code or what would amount to destruction, etc., deter third-party security researchers from undertaking activities critical for vulnerability disclosure.

[699] The only silver lining was the Aarogya Setu platform designed during Covid that was opened by the Indian government for a bug bounty program. For more details, refer to https://www.aarogyasetu.gov.in/wp-content/uploads/2020/06/mygov-999999999712190290.pdf.
[700] Section 43 imposes a penalty on a person who accesses, downloads, or introduces any computer virus, damages, disrupts, denies access, destroys, or alters the computer source code, or tampers computer resources or a network without the knowledge or consent of the owner or the person in charge.
[701] Section 65 criminalises the alteration, destruction, or concealment of the computer source code, "*which is required to be kept or maintained by law*".
[702] Section 66 criminalises any person that does any act under Section 43.
[703] Section 70 of the Information Technology Act, 2000.

The government should remove the legislative barriers by carving out an exception in the form of security research. It would entail creating a distinction between a) measures with no malicious motive, b) measures taken for research purposes or done in good faith (like transmitting malware or inserting vulnerabilities should not be penalised as the researcher has accessed and penetrated the computer source code to understand how a technology reacts when a particular malware or other vulnerability is introduced, to detect and address future risks to personal data) and c) malicious exploitation of the system, resource or network. The Indian government can learn from the Digital Millenium Copyright Act, which allows security researchers to reverse engineer a system and detect vulnerabilities. If the system is a Critical Information Infrastructure and sensitive personal details are present, it can perform a coordinated disclosure. In coordinated disclosure, the researcher only discloses the bugs in public after a reasonable opportunity has been given to the person in charge of the technology to patch the vulnerabilities. Another practice by the government can be to conduct Bug Bounty Programs, which are managed vulnerability disclosures whereby a government invites security researchers to disclose vulnerabilities in their technologies, and upon the subsequent disclosure, the researcher is rewarded.[704] Such measures can help the government create awareness about cybersecurity and privacy and incentivise future voluntary disclosures. Once legal barriers are removed, the government can harmonise the processes and infrastructural barriers and improve its interactions with security researchers.[705]

3.3. Consumer Protection Law - Product Safety and Negligence

It was essential to understand the rights available to a consumer under the Indian Consumer Protection Act (CPA), 2019 because, *firstly*, CPA imposes liability in circumstances of machine malfunctioning or design defects, thereby not limited to only products label, warranties and appearance. *Secondly*, it imposes liability on both manufacturers and sellers of the product. *Third*, it includes the mental injuries that a product can cause to a consumer, thereby expanding the scope of harm from just being physical. Furthermore, fourth, CPA provides a consumer to file a complaint both as an individual or on behalf of consumers who share common interests, thus providing a collective right of redressal. Thereby, the thesis would assert under this sub-section that CPA can serve as a useful document for the makers of the data protection law to include adequate mechanisms for grievance redressal, notwithstanding if it can be legally proved that

[704] Supra note 698.
[705] Ibid, pg. 16.

emerging technologies are a 'product' and that CPA covers 'harms' related to the different conceptualisations of the right to privacy in Chapter 2.

Artificial Intelligence technologies are a form of product or service that is subjected to children and teachers. The definition of '*person*' under the Indian consumer protection Act includes an '*artificial juridical person*'.[706] However, the legal jurisprudence regarding the liability of AI technologies is still far from reality. Historically, manufacturers, distributors, or sellers have been attributed liability for any harm caused to the buyer/consumer. In the case of semi-automated decision-making systems, i.e., where humans are in the loop for maintaining data quality or annotation, partitioning, model training, or model deployment, they can be held liable. However, when fully automated decision-making systems are deployed, the discussion around liability is murky.

The CPA does not explicitly envisage liability to the manufacturer for creating network systems or technological advancements. However, CPA defines a product as '*any article or goods or substance or raw material or any extended cycle of such product, which may be in gaseous, liquid, or solid-state possessing intrinsic value which is capable of delivery either as wholly assembled or as a part and is produced for introduction to trade or commerce*'. Artificial Intelligence technologies discussed in this thesis are solid (like CCTV cameras, RFID Smart IDs, fingerprint biometric machines or emotion/facial recognition technologies, GPS sensors, etc.) and capable of delivery as wholly assembled. Though, it can be stated that such technologies do not satisfy the requirement of '*produced for trade or commerce*' as the government is installing such technologies in schools in light of public interest. However, it is essential to note that, in most cases, the government is not producing the technologies. Instead, it procures from third-party vendors who produce for trade or commerce. Since it is established that AI technologies can be termed as '*products*', now it turns to prove who could be held liable under the Indian consumer protection regime.

Section 2(34)(v) defines '*product manufacturer*' as a person who '*designs*', produces, fabricates, '*constructs*' or re-manufactures any product '*before its sale*'. It signifies liability on the person that designs - can include a person who collects data, annotate data, and check on its data quality - and constructs - humans involved in the development stage of model testing and training, a

[706] Section 2(31), Indian Consumer Protection Act, 2019.

product. The definition of 'product manufacturer' has the potential to include humans at the design and development stages but does not signify liability for those who come in at deployment or post-deployment stage due to the inclusion of the word a *person who designs …… product before its sale*. It is where the definition of product seller holds importance. That includes *a person who, in the course of business, imports, sells, distributes, leases, installs, prepares, packages, labels, markets, repairs, maintains, and includes a service provider as well*.[707] As shown in the last chapter, the deployment stage is where the role of data scientists tends to cease, and software engineers lead, holding the mantle. The roles and responsibilities of data scientists and software engineers are not held in water-tight compartments and both work at all the stages of the AI/ML lifecycle. However, it is at deployment and post-deployment when data scientists have released the technology. It is up to the engineers and technicians to maintain/install it, distributors to sell the product, and school administrators to use it over the children. Thus, the consumer protection act seems to include the liability of persons at the design, development, and deployment stage of the product.

Now, it is proven that the technologies can be termed as products and manufacturers and sellers could be liable. Still, it remains to be discerned under what conditions or circumstances a consumer can approach the forum for redressal. The Indian CPA allows the consumer to bring action against the manufacturer or seller under two conditions, i.e. in cases of product defects called product liability and restrictive trade practices like misleading advertisements, unfair competition etc. While both are areas of concern, the former is relevant for the thesis as product defects can breach fundamental rights, including the right to privacy. '*Product liability*' means the responsibility of a product manufacturer or product seller of any product or service to compensate for any '*harm*' caused to a consumer by a defective product manufactured or sold or by a deficiency in services. Though '*harm*' does not explicitly include '*breach of privacy*', CPA defines harm as 'personal injury, death, mental agony, emotional distress' to a person.[708] Further, the word 'injury' is broad enough to encompass any harm illegally caused to anyone in mind or property.[709] Upon reading the combined definitions of product liability, harm and injury signifies three things: a) Consumers can bring claims for product liability if there is any material defect in its design, manufacture or maintenance; b) Indian CPA does not include only physical injuries but mental harms too, which as shown in previous chapters, are caused by AI technologies by way

[707] Section 2(37), Consumer Protection Act, 2019.
[708] Section 2(22), Consumer Protection Act, 2019.
[709] Section 2(23), Consumer Protection Act, 2019.

of them intruding into the intimate, secret lives of individuals or by violating their autonomy, and c) The word harm also includes 'death', which as shown in the fourth chapter in the Aadhaar context, that wrongful collection or processing of biometrics have resulted in deaths, making CPA much more comprehensive in its scope and applicability. To understand when a machine causes or could cause such harm or injuries, a consumer could utilise the fairness, transparency and accountability principles of DPIAs, audit reports or seek the Right to Explanation.

Finally, we move to the definition of the complainant under CPA, which includes a person, an organisation or association, numerous consumers sharing a common interest, legal heirs and a parent or legal guardian in case of minors.[710] It is a much wider pool of people who can seek redress than the Indian DPB, allowing only a data principal or its parent/guardian to seek grievance redressal.[711] Thus, where CPA signifies that there could be a common harm or injury from a particular product, the DPB signals that there could not be a collective claim of right to privacy. The sole condition of bringing a collective redressal claim under CPA is to seek permission from the court showing that it will benefit all consumers, and there is no requirement to seek a mandate from each consumer. It is in line with the opinion of the Advocate General of the Court of Justice of the EU, wherein he noted that "*consumer protection associations are allowed under the GDPR to institute legal action against companies without the authorisation of affected consumers where the objective of such action is to protect the rights of consumers*".[712] A collective right of redressal is fundamental in the AI context, as they are generally deployed in public settings (a private classroom is similar to a school playground or corridors as each setting/location consists of more than one child). Thus, while the harm caused to individuals will be in the form of individual bias, or a wrong prediction concerning behavioural detection, it may amplify in collective/group cases amounting to '*profiling*' and group discrimination. A collective claim of redress, whether by parents/guardians or even children (who pass the tests as shown in sections 4.1 to 4.3 of this chapter), can also bring down the trade-offs of inaccessibility, costly, time-consuming, and instead motivate the children/parents to seek redressal. Collective redressal also overpowers the information and power asymmetry between a child and parent, a child and teacher/school administration, by providing willingness and ensuring access to justice.[713]

[710] Section 2(5), read with Section 35 Consumer Protection Act, 2019.
[711] Read Section 2(6) read with Section 14 of the DPB, 2022.
[712] Court of Justice of the European Union. Advocate General's Opinion in Case C-319/20. Facebook Ireland. Press Release No 216/21 (2021) https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-12/cp210216en.pdf.
[713] Ogunleye, I. F. E. J. E. S. U. (2022). AI's Redress Problem. *CLTC White Paper Series*. Available at https://cltc.berkeley.edu/wp-content/uploads/2022/08/AIs_Redress_Problem.pdf.

CONCLUSION

Artificial Intelligence based biometric technologies and other technological measures discussed in the thesis have the potential to identify individuals and document their identity. Nishant Shah has similarly noted in the Aadhaar project landscape that it is a *'curious conflation and interoperability*' between identity and identification.[714] Shah notes that such technologies offer "*a techno-social framework where the machine function of identification is embedded into the human expression of identity*".[715] The National Academy of Science also published a report on Biometric technologies in 2010 entitled "*Biometric Recognition: Challenges & Opportunities*", which highlighted that policies should not be relied entirely on biometrics due to their probabilistic nature and should gracefully avoid violating the autonomy, dignity, and privacy of an individual. It is because of several factors:

> *"Biometric characteristics and the information captured by biometric systems can be affected by changes in age, environment, disease, stress, occupational factors, training and prompting, intentional alterations, sociocultural aspects of the situation in which the presentations occur, changes in human interface with the system, and so on. As a result, each interaction of the individual with the system (at enrolment, identification, and so on) will be associated with different biometric information.*[716]

While artificial intelligence-based biometric technologies are introduced in schools as a caring piece of technology, they often prove coercive. Due to the information asymmetry and in cases where there is no asymmetry, pressure, or want to be good in the eyes of the teacher/principal/school administration, children fear challenging the school's strategies.[717] Children lack the power, knowledge, and motivation to challenge the introduction of technologies in schools, thereby further incentivising the state to interfere with privacy boundaries rapidly. This has been the feature since Foucault's panopticon model to Surveillant Assemblage, and more so in Zuboff's Surveillant Capitalistic model, where the government cedes of its duty to protecting

[714] Shah, N. (2015). Identity and identification: The individual in the time of networked governance. *Socio-Legal Rev.*, *11*, 22.
[715] Ibid.
[716] Biometric Recognition: Challenges & Opportunities (Joseph N. Pato and Lynette I. Millett eds.), National Academy of Science- United States of America (2010).
[717] Watkins Allen, M., Coopman, S. J., Hart, J. L., & Walker, K. L. (2007). Workplace surveillance and managing privacy boundaries. *Management Communication Quarterly*, *21*(2), 172-200; Sewell, G., & Barker, J. R. (2006). Coercion versus care: Using irony to make sense of organizational surveillance. *Academy of Management Review*, *31*(4), 934-961.

privacy of students, rather intentionally allows the private players to harness personal data of students. By feeding in solutions into a data protection legislation through FATE framework, regulations focus on being child-centred by design and, by default, that respect their level of maturity, autonomy, dignity and, thereby privacy. This chapter, in its analysis, provides methodologies to the Indian judiciary, legislators and future policymakers to evaluate the complexities the emerging technologies pose.

PART A starts with examining the globally recognised principles of the rule of law, i.e., legality, necessity and proportionality principles that must be established upon any interference with the right to privacy. Such examinations occur across various emerging technologies like the traditional CCTV camera facial recognition enables technologies, biometric fingerprint scanners and highly invasive emotion recognition technologies. Though the said technologies will not be able to pass the first test of legality if challenged in courts, this chapter assumes that there is an Indian law and thereby outlines the threshold for the said principles to be considered by the courts for future cases. Part A also shows how the Indian Supreme Court went wrong in adjudging Aadhaar - a chance the court could have used to raise the standard for deploying emerging technologies. The Part proves that only some of the mentioned technologies could pass the legality, necessity, and proportionality muster.

PART B has provided a framework to the legislators and policymakers of what data protection legislation should look like. The framework embodies the principles of Fairness, Accountability, Transparency and Equity (FATE). While it looks like an overarching data protection framework meant to safeguard privacy, it applies to schools and children at the granular level. The obligations to conduct Data Protection Impact Assessment (DPIA), the obligation for data fiduciaries handling children to appoint auditors, strengthen children's right to explanation, provide matured children more autonomy from parental consent, and involve children while designing, developing, and deploying technologies, in toto, have a potential to safeguard their right to privacy. Such rights and obligations lower the information asymmetry between the child and the other stakeholders, thus providing the child with more power, knowledge, and motivation to challenge the technologies, which they presently miss in a school that is a panopticon or a surveillant assemblage.

Finally, PART C looks in detail at the Indian legislation that could serve as a reminder, caution, and act as a pillar for the Indian DPB. First, the said part starts with looking at the procurement

laws of the country, which are not specific to AI technologies, but provide a guideline for all government procurements. The chapter suggests recommendations by analysing the General Financial Rules, 2020 and WEF guidelines on procurement that advocate for more transparency in the entire procurement process that the Indian DPB should adopt. Such a transparent procurement process would allow the children or their parents/guardians to seek grievance redressal from the original equipment manufacturer collectively. Second, this part analyses Information Technology laws, whose provisions discourage third parties like ethical hackers, law firms, and academic and security researchers from understanding the black box of the technological system. The chapter shows how bug bounty programs are held globally, allowing public technological systems to be re-engineered to locate and resolve their vulnerabilities. It asserts that data security is integral to safeguarding data and, thereby, the right to privacy. Furthermore, third, the part examines the consumer protection laws, giving the children and parents individual and collective power to seek grievance redressal. Part C asserts that though consumer protection law is not meant for data protection, the DPB could use its language to protect children at all the AI/ML lifecycle stages.

This chapter appreciates that technology is being designed and deployed at a much faster scale than the legislation to regulate. In examining the different principles throughout, the chapter recommends critical learnings from the legislations and regulators from various countries like USA, UK, and EU. The chapter also emphasises that '*privacy*' and '*data protection*' are not only legal concepts and that locating answers under the legal realm would not effectively safeguard fundamental rights. Instead, the thesis novelty lies in the fact that it conducts interdisciplinary research - by understanding the domains of corporate services, financial services, data analytics, software engineering, environmental law and many others - to formulate regulations meant for child's protection of the right to privacy, and which provides power, knowledge and motivation to children to fight for their privacy rights.

CONCLUSION TO THE THESIS

The purpose and the nature of schools in present-day India sharply contrast with the schools during early post-independence India. The purpose of schools during the latter period was for nation-building and national development as an institution that imparts equality and social justice.[718] Schools were an overwhelming responsibility of the state. While providing education is still the state's responsibility, due to global aspirations and the emergence of non-state actors, education policies have shifted from state-controlled to neoliberal ones. Despite the shift towards privatisation, inequality is prevalent in Indian schools amounting to a stratified education system. The withdrawal of the state and the emergence of commercialisation in education is also marked by the growth of technologies in schools. Technologies are marketed to schools to impart security to students, provide personalised recommendations to each student, and predict children's learning engagement and dropout rate. Technologies are also perceived to remove the social barriers of caste, class, income level, sexual orientation etc. However, as the thesis shows, technology can exacerbate inequalities in a school setting.

Technologies are not merely material in nature but are cooked, i.e., defined by how they intermix with the '*practices*'. Technology ranging from a calculator to a computer to an AI technology all have relational capabilities. All technologies, as *Sacks* describe, have a '*doing*' and a '*saying*' part.[719] Every technology has a '*material*' angle, i.e. the algorithms, methods, mechanisms, and statistics captured by the '*doing*' part, and a non-technical angle, i.e. the evolving persons, motives, and situations, captured by the '*saying*' part.[720] While '*doing*' focuses on the operationalisation of any given technology, the '*saying*' describes the '*doing*' regarding how technology mediates everyday practices. Overall, the thesis's main aim has been to narrate how the right to privacy cannot be effectively safeguarded until it's analytically discussed in a context. The materiality of the technology and the embodied social practices within which technology operates constitute the '*context*'. Thus, conceptualising privacy means discussing all the '*practices*' that go into designing, developing, and deploying a technological system along with the '*materiality*' of its technical components like hardware, software, and algorithms.

[718] Nambissan, G. B., & Rao, S. S. (2013). Introduction: Sociology of education in India—Trajectory, location, and concerns. *Sociology of education in India: Changing contours and emerging concerns*, 1-23.
[719] Sacks, H. (1963). Sociological description. *Berkeley Journal of Sociology*, 1-16.
[720] Mair, M., Brooker, P., Dutton, W., & Sormani, P. (2021). Just what are we doing when we're describing AI? Harvey Sacks, the commentator machine, and the descriptive politics of the new artificial intelligence. *Qualitative Research*, *21*(3), 341-359.

The thesis relies on Helen Nissenbaum's theory of contextual integrity framework to discuss '*practices*' in an Indian school context. The framework attributes a breach of privacy to several variables present in a context, like the situation, purposes for collecting the information, the role of actors receiving the information, the position of actors providing the information, how information is transmitted, and terms and conditions of sharing the information. Once the thesis establishes that conceptualising a broader sense of privacy is futile, it describes the 'practices' in an Indian school context. By pointing out the practices of an Indian school, the thesis lays out the distinct components of a global south school that is fundamentally different from one in the global north. It affirms what *Wittgenstein* states that the right to privacy varies across cultures, periods, and geographies.[721] It pinpoints the reasons and sources where the right to privacy of a student gets lost. The discussion around practices opens the 'sites' where regulation is required to safeguard privacy effectively. For instance, the said analysis shows how the presence of information asymmetry, loss of control over information, private self-interests and false notions of political governance lead to the loss of autonomy, dignity, and integrity that constitute privacy.

While the '*practices*' describe the school setting, the stakeholders involved in the context and the available attributes to be collected, the discussion is half-baked without the fourth principle, i.e., transmission principles. Transmission principles are laid down in the context of AI-based technologies by discussing their design, development, and deployment phase, as the principles vary across stages. The thesis uses Lehr and Ohm's paper that details the various steps of and lifecycle of an Artificial Intelligence/Machine Learning system that carefully looks at each phase. Here, the thesis shows that technologies are not mere '*digital instantiations of human logic*' but are a product of several data practices.[722] Each data practice, due to its bias, inaccuracies, discrimination, lack of explainability, and other complexities, exacerbates the information asymmetries in an already stratified society leading to a loss of autonomy and dignity.

This is best shown through the case study of Aadhaar. The thesis uses Aadhaar for three primary reasons: a) It has brought India to the cusp of informational revolution by unleashing '*Digital India*', b) Its mandatory usage in schools for political governance, and c) It is an amalgam of actors who are asked to capture a variety of personal information and store in a centralised repository, all reasons contributing to the danger to the right to privacy. While Aadhaar is sold to the nation,

[721] Conceptualising Privacy, Supra note 137.
[722] Lehr and Ohm, Supra note 392, p. 717.

particularly to schools, as an instant mode of identity verification, it lowers transaction costs, eliminates fraudulent identities, and aids marginalised sections of society. However, as the thesis shows, the data practices that Aadhaar entails renders it a Panopticon. As *Ursula Rao* states, Aadhaar forms at the conjunction between machines, biological bodies, social habits, and their contexts.[723] Aadhaar is a socio-technical system that has seeped into the bureaucratic landscape, making every piece of information collected, transmitted, and stored visible to the state. As *Biswarup Sen* notes, the Aadhaar project symbolises information as societal, i.e., information is foundational to the formation of the society.[724] The Aadhaar project in schools aligns with the Digital India Programme and the National Education Policy "*to digitise all documents and records of the students and make them available on a real-time basis*". Thus, Aadhaar becomes the one-stop shop where all attributes are stored in a centralised repository. Sharing Aadhaar details with private players leads to data aggregation posing the danger of revealing critical identity details to malicious actors, turning Aadhaar into a surveillant assemblage or what *Anand Venkatnarayana* states as 360-degree databases.[725] Without data, Aadhaar would be unable to operate and therefore sees data as a capital accumulation. Such data, when transmitted across intermediaries and sold to private players, is used to profile, and target people or to model predictions. In the entire Aadhaar process, a breach of the right to privacy occurs at multiple sites, while collecting biometric data, while sharing with other government departments or private players, and at the time of yielding inaccurate predictions.

Yet, Aadhaar is not an artificial intelligence technology but rather a database that collects 360-degree information about an individual and is thereby used as a data gatherer to train AI technologies. To take the conversation forward, the thesis discusses Lehr & Ohm's various stages in the context of facial recognition, emotion recognition, fingerprinting and model predicting the dropout rates. The discussion reveals the incessant collection of sensitive personal data, including facial prints, neuro data, and financial records of the student's family. It also divulges the difference between actors involved in an Aadhaar system, like enrollment agencies, registrars, banks etc., to that of in facial recognition, which involves international players, like Microsoft, technology vendors providing learning management systems like Moodle, data scientists

[723] Rao, U. (2013). Biometric marginality: UID and the shaping of homeless identities in the city. *Economic and Political Weekly*, 71-77.
[724] Sen, B. (2020). Information and the Indian State: A Genealogy. *South Asia Multidisciplinary Academic Journal*, (23).
[725] Venkatnarayana, A., The 360-degree database, Medium, Dec 06, 2017, Available at, https://medium.com/karana/the-360-degree-database-17a0f91e6a33.

performing data training and software developers deploying the system. Thus, in the case of any given technology, privacy is outsourced to individuals or companies collecting, cleaning, training, and sharing the data.[726]

Globally, the present data protection legislation must be revised to address the abovementioned challenges. The present Indian Data Protection law rarely accounts for the 'data practices' discussed in the thesis. The judgements made by several actors as to what should be collected, cleaned, and processed to achieve their objectives yield incomplete or inaccurate predictions. The legislation in trying to curb the right to privacy remains obscure such judgements and rarely accounts for data as an asset that gets produced amidst social relations. A future legislative framework must be imaginative in understanding the emerging technological systems and account for the data disparities they create. The current notice and consent models, the rights of data subjects and the obligations of data fiduciaries must consider the socio-political condition in which data subjects provide consent, the power and knowledge asymmetry between the data subject and the data fiduciary and the control of the data subject over its information. Thus, the penultimate chapter of the thesis calls for redesigning a framework around data protection that, as a result, can safeguard the right to privacy. It calls for a framework that enhances the students' agency, gives them the power to consent, and supplies students with enough information and explanation to seek an effective grievance redressal.

The thesis adopts the FATE framework as an attempt to seal the fate of the regulatory agenda around AI systems. AI technology is inherently human from top to bottom, which involves tedious and repetitive labour.[727] Without paying attention to such human data practices, any legislative framework would be ineffective. The FATE framework allows the building of innovative and responsible data protection frameworks by considering the societal implications of AI technologies. The said framework asks the researchers to draw in interdisciplinary research with a socio-legal and technical presentation. Thus, the thesis builds an understanding of each framework principle and locates it in an Indian school context. Fairness calls for AI technology to build responsible systems by considering the societal dynamics presented in earlier thesis

[726] Waldman, A. E. (2020). Outsourcing privacy. *Notre Dame L. Rev. Reflection*, *96*, 194. Waldman uses the phrase 'outsourcing' in a context where privacy compliance is outsourced to technology vendors. The thesis uses the phrase to assert the fact that 'outsourcing' starts at the design stage itself, and continues even after the post-deployment stage.

[727] Dzeiza J., AI is a lot of work, Jun 20, Verge, 2023, Available at, https://www.theverge.com/features/23764584/ai-artificial-intelligence-data-notation-labor-scale-surge-remotasks-openai-chatbots.

sections in the form of '*practices*'. Responsibility is articulated through DPIAs that places a duty on the data controller to undergo data documentation. This in turn will also enable accountability as auditors can review the said documentation. For transparency, the thesis suggests a novel right to explanation that is absent both in the GDPR and the Indian data protection framework. The said right allows the data subject to push the data fiduciary to produce explanations suited to their needs. The thesis calls for a concise, legible, clear, and non-technical explanation. For equity, the thesis produces a three-step approach by: a) First improving the consent model in the case of children, b) Second, producing instances where parental consent does not work where 'assent' would be a way forward, and c) Third, where parental consent is the only answer, how can children be given a central role in controlling how their information is used.

The thesis believes that FATE provides a conceptual framework to regulate AI systems in a given context. It is not limited to the recommendations enlisted under each framework principle. Though, all the suggestions in the last chapter of the thesis can be practically incorporated, it is hard to say at present if they can be applied to all future AI-based technologies. Rather, it is a continuous exercise of dissecting the materiality of future technologies, analysing practices of a given specific situation, and juxtapose with the rights of data subjects to conceptualise right to privacy.

BIBLIOGRAPHY

LIST OF CASES

INDIAN CASES

FOREIGN CASES

LIST OF LEGISLATIONS/BILL

INDIAN LEGISLATIONS/BILLS

1. Companies Act, 2013
2. Constitution of India, 1950
3. Consumer Protection Act, 2019
4. Data Protection Bill, 2021
5. General Financial Rules, 2017
6. Indian Stamp Act, 1899
7. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
8. Information Technology Guidelines for Cybercafe Rules, 2011
9. Information Technology Act, 2000
10. Official Secrets Act, 1923
11. Personal Data Protection Bill, 2019
12. Right to Information Act, 2005
13. The Public Procurement Bill, 2012

FOREIGN LEGISLATIONS/BILLS

Children and Teens Online Privacy Protection Act, 1998

General Data Protection Regulation, 2016

ICO Age-Appropriate Design Code of Practice

Kids Internet Design and Safety Act, 2022

Online Harms Bill, 2023

Sarbanes Oxley Act, 2002

BOOKS

1. Althusser, L, "Ideology and Ideological State Apparatuses [1970]." *Trans. Ben Brewster. The Norton Anthology of Theory and Criticism. Ed. Vincent B. Leitch. New York: Norton* (2001).
2. Anderson, B, Census, Map, Museum, *imagined communities: Reflections on the origin and spread of nationalism*. Verso books, 2006.
3. Arjun A, '*Number in the Colonial Imagination*', in Carol Breckenridge and Peter Van Der Veer (eds) Orientalism and the Postcolonial Predicament: Perspectives on South Asia, Philadelphia: University of Pennsylvania Press, 1993.
4. Ayres, I., & Braithwaite, J. *Responsive regulation: Transcending the deregulation debate*. Oxford University Press, USA, 1995.
5. Behrent M., *Foucault and Technology*, 29 History and Technology (2013).
6. Bell A., *An Experiment in Education, made at the Male Asylum at Egmore, Near Madras: Suggesting a System by Which a School or Family May Teach Itself Under the Superintendence of the Master Or Parent* (Cadell and Davies 1805).
7. Benn S., "*Privacy, Freedom, and Respect for Persons*" in Privacy and Personality (Routledge 2017) 1-26.
8. Bentham J, and Božovič M., *The Panopticon Writings* (Verso Trade 1995).
9. Bentham J., "*Chrestomathia*" (1816) The Works of Jeremy Bentham, Vol. Eight, reprinted, New York 1-191 (1962).
10. Bentham J., "*Outline of a Work entitled Pauper Management*" in The Works of Jeremy Bentham, 1838-1843 (1797).
11. Bentham J., *Panopticon, or the Inspection House*, vol 2 (1791).
12. Bentham J., *The Collected Works of Jeremy Bentham: Constitutional Code: Volume I*, vol 1 (The Rosen Publishing Group 1983).
13. Bhatia, L., *Education and society in a changing Mizoram: The practice of pedagogy*. Vol. 1. Routledge, 2010.
14. Biometric Recognition: Challenges & Opportunities (Joseph N. Pato and Lynette I. Millett eds.), National Academy of Science- United States of America (2010).
15. Bok, S., *Secrets: On the ethics of concealment and revelation*. Vintage, 1989.
16. Brunon-Ernst A., "*Deconstructing Panopticism into the Plural Panopticons*" in Beyond Foucault (Routledge 2016).
17. Campbell C., *The Coalescent State: Assemblages of Surveillance and Public Policy*, (2020).
18. Duggan, S. AI in Education: Change at the Speed of Learning. *UNESCO Institute for Information Technologies in Education*, 2020.
19. Dworkin, Gerald. *The theory and practice of autonomy*. Cambridge University Press, 1988.
20. Edward F, *Freedom to Tinker: The Struggle to Access Devices You Own"*, Princeton University.

21. Ellul, J, John W, and Merton, R.K., *The technological society*. Vol. 303. New York: Vintage books, 1964.
22. Foucault M., *Discipline and Punish: The Birth of a Prison* (A. Sheridan trans., Penguin Books 1977) 172.
23. Foucault M., *The Foucault Effect: Studies in Governmentality* (University of Chicago Press 1991).
24. Galloway, A.R., *Protocol: How Control Exists after Decentralization*, (MIT Press 2004).
25. Gandy Jr, O.H., *The Panoptic Sort: A Political Economy of Personal Information*, Critical Studies in Communication and in the Cultural Industries (Westview Press 1993).
26. Gilligan, C., *In a different voice: Psychological theory and women's development*. Harvard University Press, 1993.
27. Goffman, Erving. *Stigma: Notes on the management of spoiled identity*. Simon and Schuster, 2009.
28. Hargreaves, D.H., *Interpersonal relations, and education*. Routledge, 2017.
29. Hastings, M., *Neoliberalism, and education*, In Oxford Research Encyclopedia of Education, 2019.
30. Heidegger M., *The Question Concerning Technology* (Harper & Row 1977).
31. Howard, P., *Beyond Punishment: Reframing Behaviour in Schools*, (CfBT Education Trust 2009).
32. Kelkar, V., & Shah, A. *In service of the republic: The art and science of economic policy*. Penguin Random House India Private Limited, 2019.
33. Kumar, K., *Social Character of Learning*. SAGE Publications India Pvt. Ltd., 1989.
34. Kupchik, A., *Homeroom Security: School Discipline in an Age of Fear*, vol 6 (NYU Press 2010).
35. Kurup, A.B., *Village, caste and education*. Rawat Publications, 2000.
36. Lazzarato, M., *Immaterial Labour* (1996) Contemporary Marxist Theory 77.
37. Lyon D., *Surveillance as Social Sorting: Computer Codes and Mobile Bodies* in David Lyon (ed), Surveillance as Social Sorting: Privacy, Risk, & Digital Discrimination (Routledge 2003).
38. Lyon D., *Surveillance Society: Monitoring Everyday Life*, McGraw-Hill Education (UK) 2001).
39. Lyon D., *The Search for Surveillance Theories*, in David Lyon (ed), Theorising Surveillance: The Panopticon and Beyond (2006).
40. Lyon, D. *Surveillance after September 11* (Vol. 11). Polity, 2003.
41. Mead, G.H., "Mind." *Self, and Society from the Standpoint of a Social Behaviorist.: University of Chicago Press: Chicago* (1934).
42. Monahan T., (ed), *Surveillance and Security: Technological Politics and Power in Everyday Life* (Taylor & Francis 2006).
43. Nagel, T, *Concealment and exposure: and other essays*. Oxford University Press, 2004.
44. Nilekani, N, *Imagining India & Ideas for the New Century*. Penguin Books India Pvt. Limited, 2008.
45. Nippert-Eng, C. E., *Islands of privacy*. University of Chicago Press, 2012.
46. Nissenbaum, Helen. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, 2009, p. 82.
47. Norris C, and Gary A., *The Maximum Surveillance Society: The Rise of CCTV*, vol 2 (Berg 1999).
48. Nussbaum C.M., *Creating Capabilities: The Human Development Approach* (Harvard University Press 2011).
49. Pasquale F, *The Black Box Society: The Secret Algorithms That Control Money and Information.* Cambridge, MA: Harvard University Press, 2015.
50. Posner, R. A., *Economic analysis of law*. Wolters Kluwer law & business, 2014.
51. Rose N., *Powers of Freedom: Reframing Political Thought* (Cambridge University Press 1999).
52. Sarangapani, M.P., *Constructing school knowledge: An ethnography of learning in an Indian village*. Sage Publications Pvt. Ltd, 2003, Jayaram, Indira. (2010).

53. Schneider B, The Hidden Battles to collect your data and control your world. New York, W.W. Norton, 2015.
54. Simon, H. A. *Models of bounded rationality: Empirically grounded economic reason* (Vol. 3). MIT press, 1997.
55. Solove, D. J. *The digital person: Technology and privacy in the information age* (Vol. 1). NYU Press, 2004.
56. Thapan, M., *Life at school: An ethnographic study*. Oxford university press, 2006.
57. Thomas, P. N. (2019). "*The Expansion of Politics as Control: Surveillance in India*" in The politics of digital India: Between local compulsions and transnational pressures. Oxford University Press.
58. Valverde M., "*Police, Sovereignty, and Law: Foucauldian Reflections*" in Police and the Liberal State (Stanford University Press 2008).
59. Wacks, R., *Personal Information: Privacy and the Law* (Clarendon Press 1993).
60. Walzer, M., *Spheres of justice: a defence of pluralism and equality*, 1984.
61. William Bogard, *Surveillance Assemblages and Lines of Flight* in Theorizing Surveillance (Willan 2006) 111-136.
62. Zuboff, S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2019).
63. Patton, M. Q. (1990). *Qualitative evaluation and research methods*. SAGE Publications, inc.
64. Bourdieu P & Wacquant J.D. Loic, An Invitation to Reflexive Sociology (1992).
65. Walzer M, Spheres of Justice: A defense of Pluralism and Equality (1983).
66. Selwyn, N., Nemorin, S., Bulfin, S., & Johnson, N. (2016). Toward a digital sociology of school. *Digital sociologies*.

JOURNALS

1. A. Acquisti. *Nudging privacy: The behavioral economics of personal information*. IEEE Security and Privacy, 7(6):82–85, 2009.
2. Acquisti, A., *Privacy in electronic commerce and the economics of immediate gratification*, (2004, May), In *Proceedings of the 5th ACM conference on electronic commerce* (pp. 21-29).
3. Acquisti, A., & Gross, R. (2009). *Predicting social security numbers from public data.* Proceedings of the National academy of sciences, *106*(27), 10975-10980.
4. Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., ... & Wilson, S. (2017). *Nudges for privacy and security: Understanding and assisting users' choices online*. *ACM Computing Surveys (CSUR)*, *50*(3), 1-41.
5. Adadi, A., & Berrada, M. (2018). *Peeking inside the black box: a survey on explainable artificial intelligence* (XAI). *IEEE access*, *6*, 138-160.
6. Aitken, V. E. (2013). An exposition of legislative quality and its relevance for effective development. *ProLaw Student Journal*, *2*, 1-43.
7. Almog, S., & Perry-Hazan, L. (2011). *The ability to claim and the opportunity to imagine: Rights consciousness and the education of ultra-Orthodox girls*. *JL & Educ.*, *40*, 273.
8. American Psychological Association Zero Tolerance Task Force, "*Are Zero Tolerance Policies Effective in the Schools? An Evidentiary Review and Recommendations*" (2008) 63 The American Psychologist 9 852.
9. Ananny, M., & Crawford, K. (2018). *Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. new media & society*, *20*(3), 973-989.
10. Andrejevic, M., & Selwyn, N. (2020). Facial recognition technology in schools: Critical questions and concerns. *Learning, Media, and Technology*, *45*(2), 115-128.
11. Arvind P, & Raghav K., *A case for a customary Right to Privacy of an Individual: A Comparative Study on Indian and other State Practice*, (2017) Oxford U Comparative L Forum 3.

12. Arvind, G.R. "Institutional context, classroom discourse and children's thinking: pedagogy re-examined." *Psicologia & Sociedade* 20, no. 3 (2008): 378-390.
13. Ashman, C.R. "The Assault on Privacy by Arthur R. Miller." *DePaul Law Review* 20, no. 4 (2015).
14. Azzarito, L., "*The Panopticon of Physical Education: Pretty, Active and Ideally White*" (2009) 14 Physical Education and Sport Pedagogy.
15. Balfanz, R., & Legters, N. (2004). Locating the Dropout Crisis. Which High Schools Produce the Nation's Dropouts? Where Are They Located? Who Attends Them? Report 70. *Center for Research on the Education of Students Placed at Risk CRESPAR*.
16. Balkin, J. (2018). Fixing Social Media's Grand Bargain. Aegis Series Paper No. 1814.
17. Balkin, J. M. (2015). Information fiduciaries and the first amendment. *UCDL Rev.*, *49*, 1183.
18. Balkin, J. M. (2017). Free speech in the algorithmic society: Big data, private governance, and new school speech regulation. *UCDL Rev.*, *51*, 1149.
19. Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *Calif. L. Rev.*, *104*, 671.
20. Barrett, L. F., Adolphs, R., Marsella, S., Martinez, A. M., & Pollak, S. D. (2019). Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements. *Psychological science in the public interest*, *20*(1), 1-68.
21. Baxi, U. (2013). Modelling "Optimal" Constitutional Design for Government Structures. *Comparative Constitutionalism in South Asia*, *28*.
22. Ben-Shahar, O., & Schneider, C. E. (2017). The failure of mandated disclosure. *Russian Journal of Economics and Law*, (4 (44)), 146-169, pp. 136
23. Berk, R. A., Sorenson, S. B., & Barnes, G. (2016). Forecasting domestic violence: A machine learning approach to help inform arraignment decisions. *Journal of empirical legal studies*, *13*(1), 94-115.
24. Bhandari, V., Kak, A., Parsheera, S., & Rahman, F. (2017). An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict. *IndraStra Global*, (11), 5.
25. Bhat, P. I. (2015). Comparative Method of Legal Research: Nature, Process and Potentiality. *Journal of the Indian Law Institute*.
26. Bhatia, G. (2014). State Surveillance and the Right to Privacy in India: Constitutional Biography. National Law School of India Review, 26(2), 127-158.
27. Big Brother Watch, "*Class of 1984: The Extent of CCTV in Secondary Schools and Academies*" (2012), London, available at: https://www.bigbrotherwatch.org.uk/files/school_cctv.pdf (consulted August 2016).
28. Birnhack, M., Perry-Hazan, L., & German Ben-Hayun, S. (2018). CCTV surveillance in primary schools: normalisation, resistance, and children's privacy consciousness. *Oxford Review of Education*, *44*(2), 204-220.
29. Black, J., & Murray, A. D. (2019). Regulating AI and machine learning: setting the regulatory agenda. *European journal of law and technology*, *10*(3).
30. Blackford, H., "*Playground Panopticism: Ring-Around-the-Children, a Pocketful of Women*" (2004) 11 Childhood.
31. Bloustein, E. J. (1964). Privacy as an aspect of human dignity: An answer to Dean Prosser. *NYUL rev.*, *39*, 962.
32. Boli, J, F. Ramirez, and J. Meyer. "Explaining the origins and expansion of mass education." *Sociological worlds: Comparative and historical readings on society* (2000): 346-354.
33. Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative research journal*, *9*(2).
34. Bracy, N. L. (2011). Student perceptions of high-security school environments. *Youth & Society*, *43*(1), 365-395.
35. Brandeis, L, and Samuel W., "The right to privacy." *Harvard law review* 4, no. 5 (1890).
36. Breiman, L. (2001). Random forests. *Machine learning*, *45*(1), 5-32.

37. Brent Daniel Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter & Luciano Floridi, The Ethics of Algorithms: Mapping the Debate, *Big Data & Society*, July–Dec. 2016, at 1–2.
38. Brill, J. (2015). Scalable approaches to transparency and accountability in decision making algorithms: remarks at the NYU conference on algorithms and accountability. *Federal Trade Commission*, *28*; Zara, C. (2015).
39. Brown, C. (2019). Critical Discourse Analysis and Information and Communication Technology in Education. In *Oxford Research Encyclopedia of Education*.
40. Calders, T., & Žliobaitė, I. (2013). Why unbiased computational processes can lead to discriminative decision procedures. In *Discrimination and privacy in the information society* (pp. 43-57). Springer, Berlin, Heidelberg.
41. Chamuah A. and Bajpai H. (2022), Towards Responsible Data Practices for Machine Learning in India: Health & Agriculture. Digital Futures Lab, Goa.
42. Cheah, P. Y., & Parker, M. (2014). Consent and assent in pediatric research in low-income settings. *BMC Medical Ethics*, *15*, 1-10.
43. Cheney, J., Chiticariu, L., & Tan, W. C. (2009). Provenance in databases: Why, how, and where. *Foundations and Trends® in Databases*, *1*(4), 379-474.
44. Christensen, L. T., & Cheney, G. (2015). Peering into transparency: Challenging ideals, proxies, and organisational practices. *Communication theory*, *25*(1), 70-90.
45. Clarke R., "*Information technology and dataveillance*" *Communications of the ACM* 31, no. 5.
46. Clarke, R., and Greenleaf, G., "*Dataveillance Regulation: A Research Framework*" (2017) 25 JL Inf. & Sci. 104.
47. Cohen, J. E. (2013). What privacy is for. *Harvard law review*, *126*(7), 1904-1933.
48. Cohen, N.S., "*The Valorization of Surveillance: Towards a Political Economy of Facebook*" (2008) 22 Democratic Communiqué.
49. Costanza-Chock, S., Raji, I. D., & Buolamwini, J. (2022, June). Who Audits the Auditors? Recommendations from a field scan of the algorithmic auditing ecosystem. In *2022 ACM Conference on Fairness, Accountability, and Transparency* (pp. 1571-1583).
50. Crain, M. (2018). The limits of transparency: Data brokers and commodification. *new media & society*, *20*(1), 88-104.
51. D'Amato, P. (2019). Simondon and the Technologies of Control: On the Individuation of the Dividual. *Culture, Theory and Critique*, *60*(3-4).
52. Dalley, P. J. (2006). The use and misuse of disclosure as a regulatory system. *Fla. St. UL Rev.*, *34*, 1089.
53. Dantcheva, A., Elia, P., & Ross, A. (2015). What else does your biometric data reveal? A survey on soft biometrics. *IEEE Transactions on Information Forensics and Security*, *11*(3), 441-467.
54. Data-in-place: Thinking through the relations between data and community. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 2863-2872).
55. Datta, A., Tschantz, M. C., & Datta, A. (2014). Automated experiments on ad privacy settings: A tale of opacity, choice, and discrimination. *arXiv preprint arXiv:1408.6491*.
56. de Zulueta, P. (2010). Choosing for and with children: consent, assent and working with children in the primary care setting. *London Journal of Primary Care*, *3*(1), 12-18.
57. Debbie VS K, "The Evolution (or Devolution) of Privacy" (2005) 20(1) *Sociological Forum* 69.
58. Deleuze, G., "*Postscript on the Societies of Control*" (1992) October.
59. Desai, S, and Veena K., "Changing educational inequalities in India in the context of affirmative action." *Demography* 45, no. 2 (2008): 245-270.
60. Diakopoulos, N. (2016). Accountability in an algorithmic decision making. *Communications of the ACM*, *59*(2), 56-62.
61. Digital inequalities in the Internet of Things: differences in attitudes, material access, skills, and usage. *Information, Communication & Society*, *24*(2).

62. Domingos, P. (2012). A few useful things to know about machine learning. *Communication of the ACM*, *55*(10), 78-87.
63. Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. *Duke L. & Tech. Rev.*, *16*, 18.
64. Eyal, O., & Roth, G. (2011). Principals' leadership and teachers' motivation: Self-determination theory analysis. *Journal of educational administration*, *49*(3), 256-275.
65. Fahlquist, J. N. (2016). Ethical concerns of using GPS to track children. In *Surveillance Futures* (pp. 122-131). Routledge.
66. Fahlquist, J. N., & Van de Poel, I. (2012). Technology and parental responsibility: the case of the V-chip. *Science and engineering ethics*, *18*, 285-300.
67. Fox, J. (2007). The uncertain relationship between transparency and accountability. *Development in practice*, *17*(4-5), 663-671.
68. Frankel, T. (1983). Fiduciary law. *Calif. L. Rev.*, *71*, 795.
69. Friedman, J. H. (1997). On bias, variance, 0/1—loss, and the curse-of-dimensionality. *Data mining and knowledge discovery*, *1*(1), 55-77.
70. Fuchs, C., "*Web 2.0, Prosumption, and Surveillance*" (2011) 8 Surveillance & Society.
71. Fuchs, M. (2008). The reliability of children's survey responses: The impact of cognitive functioning on respondent behavior. In *Proceedings of Statistics Canada Symposium* (Vol. 11, pp. 522-530).
72. Fussey, P., & Roth, S. (2020). Digitising sociology: Continuity and change in the internet era. *Sociology*, *54*(4), 659-674.
73. Gallagher, M., "*Are Schools Panoptic?*" (2010) Surveillance & Society.
74. Gavison, R. (1980). Privacy and the Limits of Law. *The Yale law journal*, *89*(3), 421-471.
75. Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Iii, H. D., & Crawford, K. (2021). Datasheets for datasets. *Communications of the ACM*, *64*(12), 86-92.
76. Gill, M., and Loveday, K., "*What Do Offenders Think About CCTV?*" (2003) Crime Prevention and Community Safety.
77. Goffman, E. (1949). Presentation of self in everyday life. *American Journal of Sociology*, *55*, 6-7.
78. Gorur, R., & Dey, J. (2021). Making the user friendly: the ontological politics of digital data platforms. *Critical Studies in Education*, *62*(1), 67-81.
79. Gross, H. (1967). The concept of privacy. *NYUL Rev.*, *42*, 34.
80. Gross, H., "The concept of privacy." *NYUL Rev.* 42 (1967).
81. Grudin, J. (2006). Turing maturing: the separation of artificial intelligence and human-computer interaction. *Interactions*, *13*(5), 54-57.
82. Guyon, I., & Elisseeff, A. (2003). An introduction to variable and feature selection. *Journal of machine learning research*, *3*(Mar), 1157-1182.
83. Hacking, I. (2015). Biopower and the avalanche of printed numbers. *Biopower: Foucault and beyond*, *65*.
84. Harry S, Machine Learning and Law, 89 WASH. L. REV. 87, 106 (2014).
85. Helen N., Privacy as Contextual Integrity, 79 WASH. LAW REV. 119, 120–121 (2004).
86. Henderson, P., Sinha, K., Angelard-Gontier, N., Ke, N. R., Fried, G., Lowe, R., & Pineau, J. (2018, December). Ethical challenges in data-driven dialogue systems. In *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 123-129).
87. Herzberg, A. (2009). Why Johnny can't surf (safely)? Attacks and defenses for web users. *computers & security*, *28*(1-2), 63-71.
88. Hoffman, A. L. (2022). Excerpt from Where Fairness Fails: Data, Algorithms, and the Limits of Antidiscrimination Discourse. In *Ethics of Data and Analytics* (pp. 319-328). Auerbach Publications.
89. Hope, A. (2010). Student resistance to the surveillance curriculum. *International Studies in Sociology of Education*, *20*(4), 319-334.

90. Hope, A. (2015). Governmentality and the 'selling' of school surveillance devices. *The Sociological Review*, *63*(4), 840-857.
91. Huan L, & Hiroshi M, Feature Extraction, Construction and Selection: A Data Mining Perspective 3-5 (1998).
92. Hutchinson, B., Denton, E., Mitchell, M., & Gebru, T. (2019). Detecting bias with generative counterfactual face attribute augmentation.
93. Johnson, D. R., & Post, D. (1996). Law and borders: The rise of law in cyberspace. *Stanford law review*.
94. Kalaiselvan, V., Kumar, P., Mishra, P., & Singh, G. (2015). System of adverse drug reactions reporting: What, where, how, and whom to report? *Indian Journal of Critical Care Medicine*, *19*(9), 564.
95. Kang J., "*Information privacy in cyberspace transactions*" Stan. L. Rev. 50.
96. Kapoor, A., & Whitt, R. S. (2021). Nudging towards data equity: The role of stewardship and fiduciaries in the digital economy. *Available at SSRN 3791845*.
97. Karst, K.L., "*The Files: Legal Controls over the Accuracy and Accessibility of Stored Personal Data*" (1966) 31(2) Law and Contemporary Problems.
98. Kasinathan, G. (2020). Making AI work in Indian education. *Artificial Intelligence in India*, *6*.
99. Khan, L. M., & Pozen, D. E. (2019). A skeptical view of information fiduciaries. *Harvard Law Review*, *133*(2), 497-541.
100. Kiener, M. (2021). When do nudges undermine voluntary consent? *Philosophical Studies*, *178*(12), 4201-4226.
101. Kopelman, L. M. (1997). The best-interests standard as threshold, ideal, and standard of reasonableness. *The Journal of Medicine and Philosophy*, *22*(3), 271-289.
102. Kumar, A. K., and Preet Rustagi. "*Elementary education in India: Progress, Setbacks, and challenges.*" (2010).
103. Laudon, K. C. (1996). Markets and privacy. *Communications of the ACM*, *39*(9), 92-104.
104. Laurence H. Tribe and Michael C. Dorf, Levels of Generality In The Definition Of Rights, 57 U. CHI. L. REV. 1057 (1990) at 1068.
105. Leff, A. A. (1970). Contract as thing. *Am. UL Rev.*, *19*, 131.
106. Lessons learned from a community-based study of infants in South India. *BMC Medical Ethics*, *12*(1), 1-9.
107. Lewis T., "The Surveillance Economy of Post-Columbine Schools" (2003) 25 Review of Education, Pedagogy, and Cultural Studies/JTL.
108. Loewenstein, G. (1996). Out of control: Visceral influences on behavior. *Organizational behavior and human decision processes*, *65*(3), 272-292.
109. Ly, B. (2017). Never Home Alone: Data Privacy Regulations for the Internet of Things. *U. Ill. JL Tech. & Pol'y*, 539.
110. Mahieu, R., & Ausloos, J. (2020). Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access.
111. Mair, M., Brooker, P., Dutton, W., & Sormani, P. (2021). Just what are we doing when we're describing AI? Harvey Sacks, the commentator machine, and the descriptive politics of the new artificial intelligence. *Qualitative Research*, *21*(3), 341-359.
112. Marda, V. (2018). Artificial intelligence policy in India: a framework for engaging the limits of data-driven decision-making. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133), 20180087.
113. Marx, L., "Technology: The Emergence of a Hazardous Concept" (2010) Technology and Culture.
114. McCahill, M, and Finn R., "*The Social Impact of Surveillance in Three UK Schools: 'Angels', 'Devils' and 'Teen Mums*" (2010) 7 Surveillance and Society ¾.

115. McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A proposal for the Dartmouth summer research project on artificial intelligence, august 31, 1955. *AI magazine*, *27*(4), 12-12.
116. McCoy, P. A. (2002). Realigning Auditors' Incentives. *Conn. L. Rev.*, *35*, 989.
117. McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *Isjlp*, *4*, 543.
118. Michael J., *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology* (Dartmouth Pub Co 1994).
119. Miglani N, and Burch P., "*Educational Technology in India: The Field and Teacher's Sensemaking*" (2019) 16 Contemporary Education Dialogue.
120. Mili. "Pedagogical reform in Indian school education: Examining the child-centred approach." *Journal of Philosophy of Education* 52, no. 3 (2018): 533-547.
121. Miller, P. B. (2013). Justifying fiduciary duties. *McGill Law Journal*, *58*(4), 969-1023.
122. Miller, P. B. (2014). Multiple loyalties and the conflicted fiduciary. *Queen's LJ*, *40*, 301.
123. Molyneux, C. S., Peshu, N., & Marsh, K. (2004). Understanding of informed consent in a low-income setting: three case studies from the Kenyan Coast. *Social science & medicine*, *59*(12), 2547-2559.
124. Moniodis C.P., "*Moving from Nixon to NASA: privacy's second strand - a right to informational privacy*" (2012) 15 Yale Journal of Law & Technology.
125. Mordini, E, and Sonia M., "Body, biometrics and identity." *Bioethics* 22, no. 9 (2008): 488-498.
126. Motwani, S., Nagpal, C., Motwani, M., Nagdev, N., & Yeole, A. (2021). AI-Based Proctoring System for Online Tests. *Available at SSRN 3866446*.
127. Murakami, D., "*What is Global Surveillance? Towards a Relational Political Economy of the Global Surveillant Assemblage*" (2013) 49 Geoforum.
128. Nambissan, G. B., & Rao, S. S. (2013). Introduction: Sociology of education in India—Trajectory, location, and concerns. *Sociology of education in India: Changing contours and emerging concerns*, 1-23.
129. Naniwadekar, M., & Varottil, U. (2016). The stakeholder approach towards directors' duties under Indian Company Law: a comparative analysis. *Mahendra Pal Singh, The Indian Yearbook of Comparative Law*, 95-120.
130. Norris, C., "*From Personal to Digital: CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control*" in Surveillance as Social Sorting (Routledge 2005).
131. O'Neil Risk Consulting & Algorithmic Auditing, Description of Algorithmic Audit: Pre-Built Assessments, Technical Report, 2020.
132. Ohm, P. (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA l. Rev.*, *57*, 1701.
133. Özpolat, G. (2020). Bringing Althusser and Foucault Together: A Brief Overview of the Question of the State. *POSSEIBLE*, (18), 7-17.
134. Page, D., "*The Abolition of the General Teaching Council for England and the Future of Teacher Discipline*" (2013) 28 Journal of Education Policy.
135. Pager, D. (2007). The use of field experiments for studies of employment discrimination: Contributions, critiques, and directions for the future. *The Annals of the American Academy of Political and Social Science*, *609*(1), 104-133.
136. Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.
137. Payne, George CF. "Making a lesson happen: An ethnomethodological analysis." The process of schooling: A sociological reader (1976): 33-40.
138. Perry-Hazan, L., & Birnhack, M. (2018). The hidden human rights curriculum of surveillance cameras in schools: Due process, privacy, and trust. *Cambridge Journal of Education*, *48*(1), 47-64.

139. Perryman, J., "*Panoptic Performativity and School Inspection Regimes: Disciplinary Mechanisms and Life Under Special Measures*" (2006) Journal of Education Policy.
140. Pound, R. (1908). *Mechanical Jurisprudence,* Columbia University Press,
141. Radin, M. (1927). The privilege of confidential communication between lawyer and client. *Calif. L. Rev.*, *16*, 487, p. 492-93.
142. Rajaraman, D., Jesuraj, N., Geiter, L., Bennett, S., Grewal, H., & Vaz, M. (2011). How participatory is parental consent in low-literacy rural settings in low-income countries?
143. Rao, U. (2013). Biometric marginality: UID and the shaping of homeless identities in the city. *Economic and Political Weekly*, 71-77.
144. Rathi A, and Tandon A., "*Capturing Gender and Class Inequities: The CCTVisation of Delhi*" (2019) Development Informatics Working Paper 81.
145. Reiman, J. H. (1976). Privacy, intimacy, and personhood. *Philosophy & Public Affairs*, 26-44, p. 35.
146. Resnick, M., Berg, R., & Eisenberg, M. (2000). Beyond black boxes: Bringing transparency and aesthetics back to scientific investigation. *The Journal of the Learning Sciences*, *9*(1), 7-30.
147. Ripken, S. K. (2006). The dangers and drawbacks of the disclosure antidote: toward a more substantive approach to securities regulation. *Baylor L. Rev.*, *58*, 139.
148. Rooney, T. (2012). Childhood spaces in a changing world: Exploring the intersection between children and new surveillance technologies. *Global Studies of Childhood*, *2*(4), 331-342.
149. Sacks, H. (1963). Sociological description. *Berkeley Journal of Sociology*, 1-16.
150. Saghai, Y. (2013). Salvaging the concept of nudge. *Journal of medical ethics*, *39*(8), 487-493.
151. Sambasivan, N., Kapania, S., Highfill, H., Akrong, D., Paritosh, P., & Aroyo, L. M. (2021, May). *"Everyone wants to do the model work, not the data work": Data Cascades in High-Stakes AI*. In *proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-15).
152. Samuelson, P. (2016). Freedom to tinker. *Theoretical Inquiries in Law*, *17*(2), 562-600.
153. Scharffs, B. G., & Welch, J. W. (2005). An analytic framework for understanding and evaluating the fiduciary duties of educators. *BYU Educ. & LJ*, 159.
154. Schmidt, A. T. (2019). Getting real on rationality—Behavioral science, nudging, and public policy. *Ethics*, *129*(4), 511-543.
155. Schnackenberg, A. K., & Tomlinson, E. C. (2016). Organizational transparency: A new perspective on managing trust in organization-stakeholder relationships. *Journal of management*, *42*(7), 1784-1810.
156. Schudson, M. (2015). *The rise of the right to know: Politics and the culture of transparency, 1945–1975*. Harvard University Press.
157. Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *NYUL rev.*, *86*, 1814.
158. Semple, J., "*Bentham's Haunted House*" (1987) 11 The Bentham Newsletter.
159. Sen, B. (2020). Information and the Indian State: A Genealogy. *South Asia Multidisciplinary Academic Journal*, (23).
160. Sengoopta, C., "Treacherous minds, submissive bodies: corporeal technologies and human experimentation in colonial India." (2018).
161. Sewell, G., & Barker, J. R. (2006). Coercion versus care: Using irony to make sense of organizational surveillance. *Academy of Management Review*, *31*(4), 934-961.
162. Shah, N. (2015). Identity and identification: The individual in the time of networked governance. *Socio-Legal Rev.*, *11*, 22.
163. Sharma, A. "Negotiating school and gender: Peer performatives." *Ethnographies of schooling in contemporary India* (2014): 21-65.

164. Shiner, R. (2005). Frederick Schauer, Profiles, Probabilities and Stereotypes. *Philosophy in Review*, *25*.
165. Siegel, S. A. (2006). The origin of the compelling state interest test and strict scrutiny. *American Journal of Legal History*, *48*(4), 355-407, p. 365.
166. Simmel, G. (1906). The sociology of secrecy and of secret societies. *American Journal of sociology*, *11*(4), 441-498.
167. Singha, R., "Settle, mobilise, verify identification practices in colonial India." *Studies in History* 16, no. 2 (2000): 151-198.
168. Solove, D. J. (2002). Conceptualising privacy. *California law review*, p. 1124.
169. Solove, D. J. (2005). A taxonomy of privacy. *U. Pa. l. Rev.*
170. Solove, D., "*Privacy and power: Computer databases and metaphors for information privacy*", Stan. L. Rev. 53.
171. Sonalde, D., Adams C, and Dubey A. "Segmented Schooling: Inequalities in Primary Education." (2009): 230-52.
172. Srinivasan, J., Finn, M., & Ames, M. G. (2015). Beyond Information Determinism to Information Orders: A New Framework for Policy. *iConference 2015 Proceedings*.
173. Stein, R. A. (2019). What exactly is the rule of law? *Houston. L. Rev.*, *57*, 185.
174. Stein, S. G. (2007). Where Will Consumers Find Privacy Protection from RFIDs? A Case for Federal Legislation. *Duke L. & Tech. Rev.*, *6*, 1.
175. Stinchcomb J.B., Bazemore G., and Riestenberg N., "*Beyond Zero Tolerance: Restoring Justice in Secondary Schools*" (2006) 4 Youth Violence and Juvenile Justice 2.
176. Stiny, G. (1980). Kindergarten grammars: designing with Froebel's building gifts. *Environment and Planning B: Planning and Design*, *7*(4), 409-462.
177. Stohl, C., Stohl, M., & Leonardi, P. M. (2016). Digital age| managing opacity: Information visibility and the paradox of transparency in the digital age. *International Journal of Communication*, *10*, 15.
178. Sukhtankar, S., & Vaishnav, M. (2015, July). Corruption in India: Bridging research evidence and policy options. In *India Policy Forum* (Vol. 11, No. 1, pp. 193-276). Delhi, India: National Council of Applied Economic Research.
179. Talib, M., "Ideology, curriculum and class construction: observations from a school in a working-class settlement in Delhi." *Sociological Bulletin* 41, no. 1-2 (1992): 81-95.
180. Taylor E, "*I Spy with My Little Eye: The Use of CCTV in Schools and the Impact on Privacy*" (2010) 58 The Sociological Review 3.
181. Taylor, M. J., Dove, E. S., Laurie, G., & Townend, D. (2018). When can the child speak for herself? The limits of parental consent in data protection law for health research. *Medical law review*, *26*(3), 369-391.
182. Tene, O., & Polonetsky, J. (2012). Big data for all: Privacy and user control in the age of analytics. *Nw. J. Tech. & Intellectual Property*, *11*, xxvii.
183. Thapliyal, N. (2012). Unacknowledged rights and unmet obligations: An analysis of the 2009 Indian Right to Education Act. *Asia-Pac. J. on Hum. Rights. & L.*, *13*, 65.
184. Thomson, J. J. (1975). The right to privacy. *Philosophy & Public Affairs*, 295-314.
185. Tickle, A. B., Andrews, R., Golea, M., & Diederich, J. (1998). The truth will come to light: Directions and challenges in extracting the knowledge embedded within trained artificial neural networks. *IEEE Transactions on Neural Networks*, *9*(6), 1057-1068.
186. Tucker, E. W. (1965). The morality of law, by Lon L. Fuller. *Indiana Law Journal*, *40*(2), 5.
187. Understanding Science Teachers' Praxis: An Ethnographic Study of Science Teaching in Four Bangalore, Schools. Doctoral Thesis, National Institute of Advanced Studies.
188. Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019, November). (Un) informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2019 ACM SIGSAC, Conference on computer and communications security* (pp. 973-990).

189. Van Dijk, T. A. (2001). Multidisciplinary CDA: A plea for diversity. *Methods of critical discourse analysis.*
190. Vanterpool, V. (2007). A critical look at achieving quality in legislation. *Eur. JL Reform*, *9*, 167.
191. Vecchione, B., Levy, K., & Barocas, S. (2021). Algorithmic auditing and social justice: Lessons from the history of audit studies. In *Equity and Access in Algorithms, Mechanisms, and Optimization* (pp. 1-9).
192. Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Colum. Bus. L. Rev.*, 494.
193. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, *7*(2), 76-99.
194. Wagstaff, K. (2012). Machine learning that matters. *arXiv preprint arXiv:1206.4656*.
195. Waits, M. R. (2016). The indexical trace: a visual interpretation of the history of fingerprinting in colonial India. *Visual Culture in Britain*, *17*(1), 18-46.
196. Waldman, A. E. (2020). Outsourcing privacy. *Notre Dame L. Rev. Réflexion*, *96*, 194.
197. Warnick, B. (2007). Surveillance cameras in schools: An ethical analysis. *Harvard Educational Review*, *77*(3), 317-343.
198. Watkins Allen, M., Coopman, S. J., Hart, J. L., & Walker, K. L. (2007). Workplace surveillance and managing privacy boundaries. *Management Communication Quarterly*, *21*(2), 172-200.
199. Welland, T., "*Living in the 'Empire of the Gaze': Time, Enclosure and Surveillance in a Theological College*" (2001) The Sociological Review.
200. Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, *25*(1), 166.
201. Wilkinson, T. M. (2013). Nudging and manipulation. *Political Studies*, *61*(2), 341-355.
202. William A. Kaplin, The Law of Higher Education 5-7 (2d ed. 1985).
203. Witten, I. H., Frank, E., & Hall, M. A. (2005). Credibility: Evaluating what's been learned. *Data mining: Practical machine learning tools and techniques*, 143-186. pp. 180.
204. Zarsky, T. Z. (2002). Mine your own business: making the case for the implications of the data mining of personal information in the forum of public opinion. *Yale JL & Tech.*, *5*, 1.
205. Zhai, X., & Renzong, Q. (2010). The status quo and ethical governance in biometrics in mainland China. In *Ethics and Policy of Biometrics: Third International Conference on Ethics and Policy of Biometrics and International Data Sharing, ICEB 2010, Hong Kong, January 4-5, 2010. Revised Papers* (pp. 127-137). Springer Berlin Heidelberg.

LIST OF REPORTS/GUIDANCES/WORKING PAPERS

1. Article 29 Data Prot. Working Party, Opinion 03/2013 on Purpose Limitation, at 47, 00569/13/EN, WP203, Available at, (Apr. 2, 2013) https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2013/wp203_en.pdf [https://perma.cc/X6PC-825X.
2. National Education Policy 2020, Ministry of Human Resource Development, Government of India.
3. A Free and Fair Digital Economy. The Committee of Experts on a Data Protection Framework for India: Justice Srikrishna Report, 2018.

4. Affective Computing The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, Available at, https://standards.ieee.org/wp-content/uploads/import/documents/other/ead1e_affective_computing.pdf.
5. Ayog, N. "Discussion Paper National Strategy for Artificial Intelligence." (2018).
6. Biometrics and Surveillance Camera Commissioner, Guidance Data protection impact assessments for surveillance cameras 22nd October 2018, Available at https://www.gov.uk/government/publications/data-protection-impact-assessments-for-surveillance-cameras.
7. Briefing Paper, CUTS International, Global Technological Developments in Age Verification and Age Estimation, 2021
8. Budget 2015-16, Speech of Arun Jaitley, Ministry of Finance, Feb 28, 2015, Available at https://www.indiabudget.gov.in/budget2015-2016/ub2015-16/bs/bs.pdf, p. 15, pp, 72.
9. Children in Scotland, '*The participation and engagement of children and young people: Our principles and guidelines*', Available at, https://childreninscotland.org.uk/wp-content/uploads/2017/11/Principles-and-Guidelines-FINAL.pdf.
10. Council of Europe, Consultative Committee of the Convention for protecting individuals concerning the automatic processing of personal data, Convention 108: Guidelines on facial recognition, 2021.
11. Department of School Education & Literacy, Ministry of Human Resource Development, Government of India, Detailed Assessment Report (NGOs and Private Organisations), 2011.
12. Department of School Education & Literacy, Ministry of Human Resource Development, Government of India, "Detailed Assessment Report (NGOs and Private Organisations), 2011, available at https://www.education.gov.in/en/sites/upload_files/mhrd/files/upload_document/Annexure%20II.pdf.
13. EDPB-EDPS Joint Opinion 5/2021 on the proposal for a regulation of the European Parliament and the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021.
14. EDPS Opinion on the use of a computerised system by the European Parliament, Available at: https://edps.europa.eu/system/files/2021-03/21-03-29_edps_opinion_ep_computerised_system_biometrics_en.pdf
15. European Commission, Proposal for a Regulation laying down harmonised rules on artificial intelligence, 21st April 2021.
16. European Union and United Nations Children's Fund, 'Module 3: Child Participation', EU-UNICEF Child Rights Toolkit: Integrating child rights in development cooperation, UNICEF Programme Division, New York, 2014. Available from: www.unicef.org/eu/crtoolkit/toolkit.html.
17. European Union and United Nations Children's Fund, 'Module 3: Child participation', EU-UNICEF Child Rights Toolkit: Integrating child rights in development cooperation, UNICEF Programme Division, New York, 2014. Available from: www.unicef.org/eu/crtoolkit/toolkit.html.
18. European Union Directorate General for Research, *An Appraisal for Technology of Political Control* - Report (EUDGR 1998), Brussels.

19. EU-UNICEF Child Rights Toolkit: Integrating child rights in development cooperation, 2014.
20. Guidance by Biometrics and Surveillance Camera Commissioner, Surveillance Camera CoP, https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-ccamera-code-of-practice-accessible-version.
21. Information Commissioner Office, Guidance to AI and Data Protection, Annex A: Fairness in the AI Life-Cycle, Available at, https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/annex-a-fairness-in-the-ai-lifecycle/.
22. Information Commissioner's Office, Guidance on AI and Data Protection, Available at, https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/how-do-we-ensure-fairness-in-ai/.
23. Lobe, B., Livingstone, S., Olafsson, K., & Simões, J. A. (2008). *Best practice research guide: How to research children and online technologies in comparative perspective*. EU Kids Online, The London School of Economics and Political Science, Available at www.lse.ac.uk/media@lse/research/EUKidsOnline/BestPracticeGuide/FAQ/FAQsReport.pdf.
24. MediaWise and United Nations Children's Fund, The Media and Children's Rights, 2nd edition, MediaWise and UNICEF, January 2005. Available from: www.mediawise.org.uk/children/the-media-and-childrens-rights.
25. National Academy of Science Report on Biometric technologies: Biometric Recognition: Challenges & Opportunities, 2010.
26. National Council for Teacher Education, National Curriculum Framework for Teacher Education, New Delhi, NCTE, 2009.
27. National Council of Educational Research and Training, National Curriculum Framework, New Delhi, NCERT, 2005.
28. Office of the High Commissioner for Human Rights, '*Guiding Principles on Business and Human Rights: Implementing the United Nations',* Protect, Respect and Remedy Framework, United Nations, New York and Geneva, 2011, Available at www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.
29. Overview of Data Protection Harms and the ICO's Taxonomy, Information Commissioner Office, April 2022, Available at https://ico.org.uk/media/about-the-ico/documents/4020144/overview-of-data-protection-harms-and-the-ico-taxonomy-v1-202204.pdf.
30. Rajya Sabha Ad-Hoc Committee Report on Pornography on social media and its effect on children and the society, 2020.
31. Report of the Joint Committee on The Personal Data Protection Bill, 2019, Seventeenth Lok Sabha, Lok Sabha Secretariat, New Delhi, December 2021.
32. Report of the UN Secretary-General, entitled The Rule of Law and Transitional Justice in Conflict and Post-Conflict Societies, 2004
33. Responses dated 31 January 2018 to the "White Paper of the Committee of Experts on a Data Protection Framework for India" dated 27 November 2017 (White Paper) released by the Ministry of Electronics and Information Technology (MeitY), Dvara Research, Available at https://www.dvara.com/research/blog/wp-

content/uploads/2018/02/Response-to-White-Paper-Public-Consultation-Dvara-Research.pdf.
34. Royal College of Pediatrics, Child Health: Ethics Advisory Committee: Guidelines for the ethical conduct of medical research involving children. Arch Dis Child 2000, 82:177–182.
35. The age of assent differs in the WHO report, World Health Organisation Research Ethics Committee: The process of obtaining informed consent, Available at http://www.who.int/rpc/research_ethics/ Process_seeking_IF_printing.pdf.
36. UNCRC (United Nations Convention on the Rights of the Child) (2021). General Comment No. 25 (2021) on children's rights in relation to the digital environment.
37. UNICEF Innocenti Research Centre, Child Safety Online: Global challenges and strategies, United Nations Children's Fund, Florence, Italy, May 2012, p. 7, www.unicef.org/pacificislands/ict_eng.pdf.
38. UNICEF Report on Engaging Stakeholders on Children Rights - A tool for companies, 2014
39. UNICEF, Engaging stakeholders on children's rights, '*A tool for companies unite for children'* First edition, Available at, https://sites.unicef.org/csr/css/Stakeholder_Engagement_on_Childrens_Rights_021014.pdf.
40. United Nations General Assembly (2021) Resolution adopted by the Human Rights Council on October 2021, 48/4, Right to privacy in the digital age.
41. United Nations Office on Drugs and Crime, '*India: Probity in Public Procurement, Transparency, objectivity and competition in Public Private Partnership projects in line with the United Nations Convention against Corruption'*, Available at, https://www.unodc.org/documents/southasia/publications/research-studies/India-PPPs.pdf.
42. World Economic Forum, AI Procurement in a box: AI Government Procurement Guidelines, Toolkit June 2020, Available at https://www3.weforum.org/docs/WEF_AI_Procurement_in_a_Box_AI_Government_Procurement_Guidelines_2020.pdf.

ONLINE ARTICLES/BLOGS

1. 5RightsFoundation. (2021, March). But how do they know it is a child? Age Assurance in the Digital World. Retrieved August 04, 2021, from 5Rights Foundation: https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf.
2. Ahuja N., & Luniya V, Introduction To Environmental, Social, And Governance (ESG) Disclosures In India With An Overview Of The Global Standards On ESG, 14th November, 2022, Available at https://www.mondaq.com/india/diversity-equity--inclusion/1250572/introduction-to-environmental-social-and-governance-esg-disclosures-in-india-with-an-overview-of-the-global-standards-on-esg.
3. Alexander, J., The Verge, Jan 6, 2020, Available at: https://www.theverge.com/2020/1/6/21051465/youtube-coppa-children-content-gaming-toys-monetization-ads.

4. B. Kiran, "*Better Data can improve public education in India - Draft National Education Policy says it too"*, The Print, 19th June, 2019. Available at https://theprint.in/opinion/better-data-can-improve-public-education-in-india-draft-national-education-policy-says-it-too/251715/.
5. Bajpai, H, The Rise of Emotiveillance? Emotion AI and Ed-Tech in India, *The Bastion*, October 12, 2020, Available at https://thebastion.co.in/covid-19/the-rise-of-emotiveillance-emotion-ai-and-ed-tech-in-india/.
6. Bajpai, H., From Moodle to Canvas: Red Flags in India's Learning Management Systems. Feb 10, 2021. Available at, https://thebastion.co.in/covid-19/from-moodle-to-canvas-red-flags-in-indias-learning-management-systems/.
7. Balaji S., *EIGHT areas where emotion AI is high-impact and high-value*, Feb 01, 2021, Available at, https://indiaai.gov.in/article/eight-areas-where-emotion-ai-is-high-impact-and-high-value.
8. Berenson, A., "*Tweaking Numbers to Meet Goals Comes Back to Haunt Executives*", N.Y. TIMES, June 29, 2002.
9. Bhatia, G., "*The Right to Privacy and the Supreme Court's Referral: Two Constitutional Questions*", August 11, 2015, Indian Constitutional Law and Philosophy. Available at https://indconlawphil.wordpress.com/2015/08/11/the-right-to-privacy-and-the-supreme-courts-referral-two-constitutional-questions/ (Accessed on 19th January, 2021).
10. Bhatty, K., "*The Numbers Game: How Well has it served the cause of Education?*", The Print, April 14, 2018. Available at https://www.epw.in/journal/2018/15/insight/numbers-game.html.
11. Bianca B., Facebook Privacy Policy Explained: It's Longer Than The Constitution, Huffington Post (July 12, 2010), online at http://www.huffingtonpost.com/2010/05/12/facebookprivacy-policy-s_n_574389.html. Facebook's privacy policy contains more words - 5830 - than the U.S. Constitution.
12. Brandom R., Facebook shut down German research on an Instagram algorithm, researchers say, August 13, 2021, Available at, https://www.theverge.com/2021/8/13/22623354/facebook-instagram-algorithm-watch-research-legal-threat.
13. C. Julie, Scaling Trust and Other Fictions, *Law and Political Economy*, 29th May, 2019. Available at, https://lpeproject.org/blog/scaling-trust-and-other-fictions/.
14. CCTV Could Be Used in Exam Rooms" (BBC News, April 11, 2008), available at: http://news.bbc.co.uk/1/hi/education/7342432.stm.
15. Central Board of Secondary Education, Circular Number, 19/2017, Safety of Children in Schools, Available at: https://www.cbse.gov.in/cbsenew/Examination_Circular/2017/16_CIRCULAR.pdf.
16. China has restricted children's usage of online gaming apps: https://www.cnbc.com/2021/08/30/china-to-ban-kids-fromplaying-online-games-for-more-than-three-hours-per-week.html.
17. D. Vincy, "*Why Delhi's government school teachers feel they are not doing the job they were hired for"*, The Print, 25th June, 2019, Available at, https://theprint.in/opinion/why-delhis-government-school-teachers-feel-they-are-not-doing-the-job-they-were-hired-for/254061/.
18. DT Next, TN to launch all in one portal to track schools, 26th May, 2019, Available at https://www.dtnext.in/News/TopNews/2019/05/26045928/1139624/TN-to-launch-allinone-portal-to-track-schools.vpf.
19. Dzeiza J., AI is a lot of work, Jun 20, Verge, 2023, Available at, https://www.theverge.com/features/23764584/ai-artificial-intelligence-data-notation-labor-scale-surge-remotasks-openai-chatbots.
20. Economic Times Tech, *200 agencies to enroll citizens for UID*, Jul 16, 2010, Available at, https://economictimes.indiatimes.com/tech/software/200-agencies-to-enroll-citizens-for-uid/articleshow/6173502.cms?from=mdr.
21. Express Desk, "Ryan Murder Case: CCTVs, Verification of Staff among Rules CBSE has Issued for Schools" (Indian Express, September 14, 2017), available at:

https://indianexpress.com/article/education/ryan-murder-case-cbse-issues-safety-guidelines-to-schools-gurugram/.
22. From April 1, 2021, the Punjab Schools are obliged to undergo Aadhaar biometric updation from primary school students to senior secondary school students. Available at https://www.tribuneindia.com/news/schools/punjab-school-education-department-directs-for-biometric-updation-in-aadhaar-cards-of-students-226135.
23. G. Lauryn, G.C.J, L. Peter, S. Kent et al., How to select algorithms for Azure Machine Learning. Available at https://docs.microsoft.com/en-us/azure/machine-learning/how-to-select-algorithms.
24. G.S. Swati, Data of 78,000 Maharashtra students goes missing, ToI, Jun 1, 2021. Available at, https://timesofindia.indiatimes.com/home/education/news/data-of-78000-maharashtra-students-goes-missing/articleshow/83128536.cms.
25. Greater Kashmir, "In J&K government schools, flawed UDISE data hampers infrastructure upgradation", 19th May 2018. Available at, https://www.greaterkashmir.com/kashmir/in-jk-govt-schools-flawed-udise-data-hampers-infrastructure-upgradation.
26. Greater Kashmir, "*In J&K government schools, flawed UDISE data hampers infrastructure upgradation*", 19th May 2018. Available at https://www.greaterkashmir.com/kashmir/in-jk-govt-schools-flawed-udise-data-hampers-infrastructure-upgradation.
27. H. Rebecca, YouTube's kids app has a rabbit hole problem, Vox, May 12, 2021, Available at, https://www.vox.com/recode/22412232/youtube-kids-autoplay.
28. India Today, July 2, 2020, Available at https://www.indiatoday.in/mail-today/story/installation-of-1-4-lakh-chinese-cctv-cameras-by-delhi-govt-sparks-row-1696032-2020-07-02.
29. Indian Express, *NEP roll-out,* October 15, 2020, Available at, https://indianexpress.com/article/education/education-ministry-world-bank-launch-rs-5718-crore-project-to-improve-school-education-in-6-states-6724978/.
30. J. Isha, "Incomplete data hits University Grants Commission", ToI, Mar 25, 2011. Available at, https://timesofindia.indiatimes.com/city/lucknow/incomplete-data-hits-university-grants-commission/articleshow/7784223.cms.
31. Jain, A., *Hey CM, Leave these Kids alone*, Internet Freedom foundation, 30th July 2022, Available at, https://internetfreedom.in/hey-cm-leave-those-kids-alone/.
32. K. Sharvari, "Using Data to Improve how social-emotional learning is measured", The Bastion, May 26, 2022. Available at, https://thebastion.co.in/politics-and/education/using-data-to-improve-how-social-emotional-learning-is-measured/.
33. K. Shyna, Teachers turning YouTube into education platform amid lockdown, *Indian Express*, April 26, 2020, Available at: https://indianexpress.com/article/education/teachers-turning-youtube-into-education-platform-amid-lockdown-and-how-you-can-do-it-too-6371382/.
34. Kaveri M, The News Minute, Aug 10, 2019, Available at, https://www.thenewsminute.com/article/tn-govt-makes-aadhaar-enrolment-compulsory-school-students-sparks-row-107004.
35. Kumar, M., The Hindu, Sept 26, 2022, Available at, https://www.thehindu.com/news/national/other-states/dalit-student-dies-after-being-beaten-by-teacher-opposition-mounts-pressure-on-government-for-action/article65937441.ece.
36. Levine A., Chilling': Facial recognition firm Clearview AI hits watchdog groups with subpoenas, Politico, 24th September 2021, Available at, https://www.politico.com/news/2021/09/24/clearview-ai-subpoena-watchdog-groups-514273;
37. M. Diepeu, Strengthening Data Quality: A step to resolve education debacle, Nagaland Post, July 7, 2021. Available at https://www.nagalandpost.com/index.php/strengthening-data-quality-a-step-to-resolve-edn-debacle/.
38. Moneylife Digital Team, *UIDAI not so clean partners and their tainted executives*, 15th November, 2010, Available at, https://www.moneylife.in/article/uidais-not-so-clean-partners-and-their-tainted-executives/.

39. Murali, A, *The Big Eye: The tech is all ready for mass surveillance in India,* Factor Daily, Aug 13, 2018, Available at https://factordaily.com/face-recognition-mass-surveillance-in-india/.
40. Naraharisetty R., "Casteism still thrives in elite schools in India. What would Anti-Caste Education Look Like?", Swaddle, July 14, 2021. Available at https://theswaddle.com/casteism-still-thrives-in-elite-schools-in-india-what-would-anti-caste-education-look-like/.
41. On August 2, 2019, the school education department of Tamil Nadu through a circular pushed for Aadhaar enrolment for school students under the "*Samgra Shiksha Abhiyan*" which covers 58,474 schools and over 1.23 crore students. Available at https://www.eastmojo.com/news/2020/11/09/free-aadhaar-cards-for-assam-school-students/.
42. Pain, R., Whitman, G., & Milledge, D. (2011). Participatory action research toolkit. Available at https://www.durham.ac.uk/media/durham-university/research-/research-centres/social-justice-amp-community-action-centre-for/documents/toolkits-guides-and-case-studies/Participatory-Action-Research-Toolkit.pdf.
43. Persily, N., Facebook hides data showing it harms users. Outside scholars need access', October 5, 2021, Available at https://www.washingtonpost.com/outlook/2021/10/05/facebook-research-data-haugen-congress-regulation/.
44. Privacy International (Nov. 8, 2018), http://privacyinternational.org/advocacy-briefing/2426/our-complaints-against-acxiom-criteo-equifaxexperian-oracle-quantcast-tapad.
45. Roy, S., & Uday, D. (2020, August). Does India need a public procurement law? The Leap Blog, available at: https://blog.theleapjournal.org/2020/08/does-india-need-public-procurement-law.html#gsc.tab=0.
46. RTE Linked to Aadhaar to avoid duplication, The Times of India, Feb 28, 2018, Available at, https://timesofindia.indiatimes.com/city/bengaluru/rte-linked-to-aadhaar-to-eliminate-duplication/articleshow/57381223.cms.
47. Sarita, S., '*Indian Police use facial recognition to persecute Muslims and other marginalised communities*', 11th October 2022, Available at https://www.codastory.com/authoritarian-tech/india-police-facial-recognition/.
48. School Head Defends Toilets CCTV" (BBC News, January 27, 2009), available at: http://news.bbc.co.uk/1/hi/wales/mid/7851282.stm.
49. Sharma A., Govt. *plans to limit role of private agencies in Aadhaar enrolment*, Economic Times Politics, Sep 08, 2017, Available at, https://economictimes.indiatimes.com/news/politics-and-nation/government-plans-to-limit-role-of-private-agencies-in-aadhaar-enrolment/articleshow/60415970.cms?from=mdr.
50. Sharma R, and Raja A., "Gujarat's New System of Teacher Attendance" (September 7, 2019) Indian Express, available at: https://indianexpress.com/article/explained/explained-gujarat-new-system-of-teachers-attendance-through-face-recognition-5975585/.
51. Sharma R., *Teacher, student, schools to be tracked*, Indian express, Sept 19, 2020, Available at, https://indianexpress.com/article/education/gujarat-teachers-students-schools-to-be-tracked-to-analyse-online-classes-6601875/.
52. Sharma, R., Facial Recognition Attendance System in Gujarat, Indian Express, Available at: https://indianexpress.com/article/education/facial-recognition-attendance-system-it-is-fool-proof-has-no-scope-for-manipulation-says-education-secretary-5925570/.
53. Sunil MK, Govt schools get smart with RFID Badge in Kerala, Aug 13, 2015, Available at https://timesofindia.indiatimes.com/city/kochi/Govt-schools-get-smart-with-RFID-badge-in-Kerala/articleshow/48465037.cms.
54. Teachers Watched on CCTV Cameras" (BBC News, March 4, 2009), available at: https://www.bbc.co.uk/news/uk-scotland-tayside-central-21716049.
55. The Hindu, *E&Y selected as consultant for UIDAI*, Feb 26, 2010, Available at, https://www.thehindu.com/news/national/Ernst-and-Young-selected-as-consultant-for-UIDAI/article16817121.ece.

56. The Hindu, *Purchase of school IT equipment: rates revised in guidelines*, Feb 19, 2022, Available at https://web.archive.org/web/20220220063946/https://www.thehindu.com/news/national/kerala/purchase-of-school-it-equipment-rates-revised-in-guidelines/article65066399.ece.
57. Under *Axom Sarba Siksha Abhijan Mission*, the process of distribution of free Aadhar cards has started under which, if any student has an Aadhaar number can avail of services of a free bank account. Available at https://www.eastmojo.com/news/2020/11/09/free-aadhaar-cards-for-assam-school-students/.
58. Venkatnarayana, A., The 360 degree database, Medium, Dec 06, 2017, Available at, https://medium.com/karana/the-360-degree-database-17a0f91e6a33.
59. Yadav A., *Parents struggle to sign up infants*, Identity Project, Aug 29, 2016, Scroll, Available at, https://scroll.in/article/814891/parents-struggle-to-sign-up-infants-toddlers-for-aadhaar-as-centre-eyes-100-enrolment-by-march.