Retaining informational privacy in the age of emerging technology

February 2022

Vidhi Centre for Legal Policy

This working paper is a non-commissioned report prepared by the Centre of Applied Law & Technology Research (ALTR), at the Vidhi Centre for Legal Policy, an independent think-tank doing legal research to help make better laws and improve governance for the public good.

About the authors

Dhruv Somayajula is a Research Fellow working with the Centre for Applied Law & Technology Research (ALTR) at Vidhi. Ameen Jauhar is a senior resident fellow at Vidhi, and the team lead for ALTR.

The authors acknowledge the excellent research assistance provided by our intern Dhruv Holla (National Law School of India University).

.

Retaining informational privacy in the age of emerging technology

Introduction

Emerging technologies refer to novel fast-growing technologies that are emerging into prominence, and whose potential for impact is, to a large extent, unrealized in the present.[1] The twenty-first century has seen a rapid rise in the deployment of several emerging technologies such as artificial intelligence (AI), cryptocurrency, metaverse, non-fungible tokens (NFTs) and the Internet of Things (IoT). In contrast to concepts such as metaverse and NFTs that are quite nascent in 2022, mainstream acceptance and adoption of AI and IoT technologies has been observed across the world. The use of AI systems and IoT devices in human-facing interactions have enabled greater personalization and greater capabilities in medicine[2], education[3], healthcare[4] and law enforcement[5] through the use of personal data.[6]

However, these emerging technologies raise unique concerns to the right to informational privacy, which is a facet of the right to privacy guaranteed by Article 21 of the Constitution. Due to concerns regarding stifling innovation, emerging technologies are not subject to unduly hasty regulation.[7] However, waiting for an emerging technology to mature into the market and become mainstream, in the absence of any governance oversight, has its own downsides. In such a scenario, the law is perennially playing a catching-up game to the consequences of technologies.[8] It is feasible to record and

[1] Daniele Rotolo et al, 'What is an emerging technology?' (2015) Research Policy <https://core.ac.uk/download/30612882.pdf> accessed 10 January 2022
[2] Anita Borges, Lakshmi Krishnan, 'AI can make breast cancer screening more accessible and affordable' (15 November 2021) World Economic Forum <https://www.weforum.org/agenda/2021/11/ai-breast-cancer-screening-more-accessible-and-affordable/> accessed 10 January 2022
[3] 'How is AI transforming the education industry' (28 June 2021) Data Quest <https://www.dqindia.com/ai-transforming-education-industry/> accessed 10 January 2022
[4] 'Internet of things (IOT) in Healthcare Market to Reach Over $190 Billion by 2028 – Powered by Increasing Implementation of Cloud Computing - Exclusive Report by Vantage Market Research' (26 January 2022) GlobeNewswire < https://www.globenewswire.com/news-release/2022/01/26/2373724/0/en/Internet-of-things-IOT-in-Healthcare-Market-to-Reach-Over-190-Billion-by-2028-Powered-by-Increasing-Implementation-of-Cloud-Computing-Exclusive-Report-by-Vantage-Market-Research.html> accessed 4 February 2022
[5] ANI, 'Madurai Police Launches Facial Recognition App To Reduce Crime Rate' (Tamil Nadu, 26 September 2020) NDTV <https://www.ndtv.com/tamil-nadu-news/madurai-police-launches-facial- recognition-app-facetagr-to-reduce-crime-rate-2301538> accessed 23 January 2022; HT Correspondent, 'Patiala Police nab 2 criminals using face recognition app' (Patiala, 1 June 2020) Hindustan Times <https://www.hindustantimes.com/chandigarh/patiala-police-nab-2-criminals -using-face-recognition-app/story-ZiGYD3Bh0GzUbSPls5S2JJ.html> accessed 23 January 2022
[6] Raphaël Gellert, 'Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies' (2021) 11(2) International Data Privacy Law <https://academic.oup.com/idpl/article/11/2/196/6071468> accessed 2 February 2022
[7] Tom Relihan, 'Will regulating big tech stifle innovation?' (27 September 2018) MIT Management Sloan School <https://mitsloan.mit.edu/ideas-made-to-matter/will-regulating-big-tech-stifle-innovation> accessed 23 January 2022
[8] Daniel Malan, 'The law can't keep up with new tech. Here's how to close the gap' (21 June 2018) World Economic Forum <https://www.weforum.org/agenda/2018/06/law-too-slow-for-new-tech-how-keep-up/> accessed 13 January 2022

analyse potential concerns raised by emerging technology in the initial course of its operation to lay the groundwork for an informed and timely regulatory framework.

The Personal Data Protection Bill, 2019 (PDP Bill 2019) was proposed to set out a legal framework for informational privacy and data protection. It primarily seeks to regulate personal data collection and processing. In light of the recent recommendations by the Joint Parliamentary Committee on the PDP Bill 2019, a revised version may be tabled before the Parliament in the near future. Given that certain emerging technologies heavily rely on personal data processing, this is an opportune moment to examine the provisions of the PDP Bill 2019 in light of these features.

It is complicated to predict the exact types of consequences and negative effects of an evolving technological innovation. However, based on limited deployments seen across the world and specifically within India, this paper seeks to examine the concepts of privacy, autonomy, meaningful consent, and regulatory frameworks that preserve informational privacy in this era of emerging technologies. The paper does not discuss the use of non-personal data by emerging technologies. As such, all references to data processing within this paper relate to personal data being processed by data fiduciaries. Lastly, references to emerging technology for the purposes of this paper are limited to human-facing AI and IoT technologies and is not a sweeping comment for all emerging technologies. This has been done in order to retain the focus on informational privacy and the exercise of autonomy, as elaborated in Part 2.

This paper is divided into the following parts. Part 1 of this paper introduces the right to (informational) privacy, and its relation to control over one's data. It discusses the notice-and-consent framework and its importance to meaningful consent. Part 2 of this paper looks at the emergence of AI and IoT and discusses the risks associated with them around informational privacy. Part 3 of this paper discusses the merits of a regulatory approach involving rights and baseline obligations to supplement the notice-and-consent model. Further, Part 3 analyses various provisions of the PDP Bill 2019 through the lens of preserving informational privacy. Lastly, Part 4 points out the limitations in the PDP Bill regarding certain applications of emerging technologies needing to be addressed.

I. *Puttaswamy*, privacy and informed consent:

A. Puttaswamy and informational autonomy

The Supreme Court, in *Justice KS Puttaswamy (Retd.) v. Union of India*, recognised the right to privacy within Article 21 of the constitution.[9] The Court acknowledged the risks with inadequate protection of personal data resulting in issues of profiling through aggregation of personal data and individuals being constantly open to electronic scrutiny.[10] It further recognised the right to *informational privacy* as a facet of the right to privacy.[11] In doing so, the Court has brought in protection of information (data protection) as a necessary component of the right to privacy, and framed the issue of privacy specifically around the processing of personal data. This case marks the recognition of data protection, and acknowledges the importance of one's data being reflective of one's *persona* and *identity*. *Puttaswamy* also discusses the impact of emerging technology and their accelerated features of data gathering and data processing, which further create deeper profiles of their users and increase concerns of privacy.[12] In the digital age, the right to privacy is also to be understood as the right to protect one's identity.[13]

However, the mere recognition of what comprises the individual's right would render any discourse on personal data protection a non-starter. For a right to be meaningfully engaged with, it is necessary to look at who wields this right and within what limits. *Puttaswamy* takes this discussion forward and locates the right to informational privacy within the individual, tying the idea of personally identifiable data about a person to the inherent identity of the person.[14] This link formally introduces the concept of *informational autonomy* to the Indian legal jurisprudence.[15] In this regard, the Court had much help from contemporary legal standards across the world that recognised a similar line of thought.[16] The idea of informational autonomy, condensed to its minimum, is that an individual is entitled to freely determine the treatment of their personal information vis-à-vis any other entity.[17] The pre-eminence granted to the individual and their free and informed consent to share personal information, thus, assumes centre stage. Even where exceptions are carved into the exercise of this right, as evolved within *Puttaswamy*, consent plays a key role.[18]

---

[9] Justice KS Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
[10] Para 170-171, Part S of judgment authored by Chandrachud J.
[11] Para 172, ibid
[12] Para 174, ibid refers to 'internet of things, metadata, wearable devices and social media networks'
[13] Para 177, ibid
[14] Ibid
[15] "Privacy postulates the reservation of a private space for the individual, described as the right to be let alone. The concept is founded on the autonomy of the individual" Part R, Puttaswamy (2017)
[16] Yvonne McDermott, 'Conceptualising the right to data protection in an era of Big Data' (2017) Big Data & Society <https://doi.org/10.1177/2053951716686994> accessed 15 January 2022
[17] Anuj Garg v. Hotel Assn. of India [(2008) 3 SCC 1] para 34-35; "Privacy has distinct connotations including (i) spatial control; (ii) decisional autonomy; and (iii) informational control"; Paras 141,177, Part L, Puttaswamy (2017)
[18] John Sebastian, Aparajito Sen, 'Unravelling The Role Of Autonomy And Consent In Privacy' (2020) Indian Journal of Constitutional Law <https://ijcl.nalsar.ac.in/wp-content/uploads/2020/08/9IndianJCon stL1_SebastianSen.pdf> accessed 20 January 2022

Consent is universally recognized as a key to exercising informational autonomy.[19] However, the textual reverence to consent is often followed by confused multi-directional attempts to understand how to operationalise this key point. Consent plays a role in a data processing ecosystem akin to a switch, i.e., consent, or its lack thereof, allows individuals and companies to make decisions on whose personal data may or may not be processed. In this context, the following section analyses the role of notice-and-consent framework to facilitate meaningful consent.

B. Notice and consent framework

(a) *How it works:*

The 'notice-and-consent' framework involves the receipt of notice by a data principal regarding their personal data sought to be collected by a data fiduciary, for which they can give their consent.[20] This is a contractarian sequence which assumes the ability of a user to give 'meaningful consent'.[21] Personal data gathered by various digital operators is seen as a commodity provided by the user. This data may be used for targeted advertising, campaigning, profiling, recommendations based on interests and past activities etc.[22] Digital operators see the value in users appreciating personalised recommendations and services, which further incentivizes the use of more personal data and data gathering in general to provide greater value to the consumers. Online advertisers offer lucrative deals to digital operators for this personal data. The cumulative commercial role played by a user's personal data, individually or aggregated, reflects the contractarian approach to personal data. Its commodification as a resource of tremendous value has resulted in personal data being treated as 'consideration' in a contract. In this regard, consent is not merely taken as a matter of form, but must be given in a substantive manner.[23] The notice-and-consent framework facilitates this by requiring the user to be informed through a notice displayed on their screen. If the user consents to the data being processed or clicks on the icon marked 'I Agree', they are presumed to have consented to the notice that was displayed on their screen.

(b) *Approaches to soliciting consent:*

[19] Puttaswamy, para 171; Ibid
[20] Daniel Solove, 'Privacy Self-Management and the Consent Dilemma' (2012) 126 Harvard Law Review <https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf> accessed 20 January 2022
[21] Pamela Samuelson 'Privacy As Intellectual Property?' (2000) 52(5) Stanford Law Review <https://www.researchgate.net/publication/228188988_Privacy_As_Intellectual_Property> accessed 21 January 2022
[22] Issie Lapowsky, 'How Cambridge Analytica Sparked the Great Privacy Awakening' (17 March 2019) *WIRED* <https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/> accessed 21 January 2022
[23] This is reflective of the requirement of substantive consent evolved in medical contexts, through the use of 'informed consent' forms for clinical trials. See Elaine Sedenberg, Anna Lauren Hoffmann, 'Recovering the History of Informed Consent for Data Science and Internet Industry Research Ethics' (2016) SSRN Electronic Journal <https://arxiv.org/ftp/arxiv/papers/1609/1609.03266.pdf> accessed 18 January 2022

Data protection law is generally based on the market approach or the regulatory approach to personal data.[24] On its face, these approaches look varied. The market approach focuses on the competitive nature of the market and the individual choices made by a rational consumer. On the other hand, the regulatory approach focuses on a notice-and-consent framework that relies on taking a compliance-based governance approach to personal data, where the state forbids certain data processing or adds additional conditions to data processing for the welfare of the individual.

The regulatory approach is decidedly not an individualistic approach. However, it has practical merit. In today's age of privacy policies and standardised contracts, users are presented with a 'take it or leave it' conundrum. There is no room for negotiation or individual alteration of contractual terms between a digital service provider and a user. The user is then either forced to consent to all of the terms whether or not they understand and agree to them, or to leave the service. In this case, the individual does not have the bargaining power to change the digital operator's planned data processing behaviour. On the other hand, the state, as a regulating agency, has the power to enforce such behavioural changes through ring-fencing data from being processed for certain purposes or to require additional compliances for data processing. For example, WhatsApp attempted to introduce certain terms and conditions that made it mandatory for users to share certain meta data with WhatsApp's parent company Facebook Inc., failing which their accounts would be suspended. However, sustained public opposition along with governmental intervention successfully led to WhatsApp indefinitely deferring their deadlines to operationalise these unilateral changes to its terms and conditions.[25]

(c) *Meaningful consent:*

The notice-and-consent framework shows an overlap between the market approach and the regulatory approach through its most important feature, namely its emphasis on meaningful consent. Per the market approach to data protection, consent must be given from the perspective of a rational consumer making a conscious choice.[26] The choice must be an informed choice to avoid externalities such as informational asymmetry distorting the market conditions for this trade-

[24] John Sebastian, Aparajito Sen, 'Unravelling The Role Of Autonomy And Consent In Privacy' (2020) Indian Journal of Constitutional Law <https://ijcl.nalsar.ac.in/wp-content/uploads/2020/08/9IndianJCon stL1_SebastianSen.pdf> accessed 20 January 2022
[25] Aashish Aryan, 'WhatsApp defers May 15 deadline on privacy policy' (9 May 2021) *The Indian Express* <https://indianexpress.com/article/technology/social/whatsapp-scraps-may-15-deadline-for-accepting-new-privacy-policy-terms-7306026/> accessed 5 February 2022
[26] Robert Sloan, Richard Warner, 'Beyond Notice and Choice: Privacy, Norms, and Consent' (2013) SSRN Electronic Journal <http://dx.doi.org/10.2139/ssrn.2239099> accessed 19 January 2022

off.[27] In this regard, the framework of notice-and-consent theoretically enables the user to understand what they are consenting to, through the notice received by the user prior to giving consent.

However, on the other end of the spectrum, privacy and data protection can also be understood as facets of human rights and individual dignity.[28] In this regard, one's personal data is not just seen as a commodity that can enrich others, but firstly as a facet of the user's identity and a personal identifier.[29] The question of processing another person's personal data then raises issues against commodifying aspects of their identity and personality.[30] This issue sees some resolution through the individual's control over their right to consent to who can process their information within what limits. This control is exercised by the individual through their consent for processing of their personal data. However, the individual is not truly in control of the end use of their information if their consent has been obtained under false or deceptive pretexts. Accordingly, the consent granted from a rights-based perspective must also be a meaningful consent derived out of adequate information.

(d) *Is notice-and-consent enough?*

We have discussed that meaningful consent is indeed at the root of any processing of personal data, regardless of whether that personal data is seen as a tradeable commodity or as an extension of one's persona. Most data processing today follows the notice-and-consent framework.[31] This model has been replicated over the years through regulatory pushes across the world.[32] The global approach towards these provisions indicates universal agreement that the notice-and-consent framework is the ideal framework to secure meaningful consent, and as a result, achieve informational privacy alongside technological progress.

These questions are all the more relevant in dealing with recent issues highlighted by the digital sphere. For example, individuals may claim to highly value privacy as an abstract concept, but undertake very little in behavioural terms to protect their information online.[33] Such behaviour has been attributed to the inability to

[27] Ibid
[28] Edward J. Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 NYU Law Review; see also Puttaswamy at para 171
[29] Yvonne McDermott, 'Conceptualising the right to data protection in an era of Big Data' (2017) Big Data & Society <https://doi.org/10.1177/2053951716686994> accessed 15 January 2022
[30] Cameron Kerry, John Morris Jr., 'Why data ownership is the wrong approach to protecting privacy' (26 June 2019) *Brookings* <https://www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/> accessed 19 January 2022
[31] FH Cate, Viktor Mayer-Schönberger, 'Notice and consent in a world of Big Data' (2013) 3(2) International Data Privacy Law <http://dx.doi.org/10.1093/idpl/ipt005> accessed 24 January 2022
[32] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980; Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market
[33] Abhishek Gupta et al, 'The Privacy Conundrum: An empirical examination of barriers to privacy among Indian social media users' to be published. ; see also Helen Nissenbaum, *Privacy in context: Technology, policy, and the integrity of social life* (2009) Stanford

cognitively process information collection through computers, wrong estimation of risks, and desires for immediate gratification.[34] This discrepancy between their behaviour, also called the 'privacy paradox', raises questions on whether 'notice-and-consent', often taken at the first point of data collection, is enough to represent meaningful consent.[35] Further, in addition to user behaviour, platform behaviour can also weaken the meaningfulness sought to be ensured by notice-and-consent frameworks. For example, deliberate attempts to direct users to pick one option over the other through the use of colour, harmless words, and making exercise of privacy-conscious behaviour difficult may all be seen as examples of dark patterns.[36] These designs expose the vulnerability of notice-and-consent frameworks in ensuring meaningful consent.

Similarly, recent technological developments, popularly termed *emerging technologies*, raise questions on whether notice-and-consent can adequately ensure meaningful consent. More importantly, can meaningful consent by itself adequately protect the right to informational privacy? Lastly, if meaningful consent by itself cannot adequately ensure informational privacy, what can be added to ensure the protection of this constitutional right?

II. Emerging technology and issues posed to meaningful consent

These questions may be answered by looking at the features unique to emerging technologies that threaten our current notions of informational privacy. Over the years, technological innovations have been intertwined with the processing of personal data in an attempt to increase accuracy and specificity.

Emerging technologies aim to increase capabilities, accuracy and efficiency by computing, processing and analysing vast data corpuses.[37] This data often includes large amounts of personal data for those emerging technologies that directly interact with humans for their functionality.[38] The most prominent emerging technologies operating in this field are the Internet of Things (IoT) and artificial intelligence systems. These technologies are

University Press

[34] Susanne Barth, Menno D.T.de Jong, 'The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review' (2017) 34(7) Telematics and and Informatics <https://www.sciencedirect.com/science/article/pii/S0736585317302022> accessed 24 January 2022

[35]

[36] Sara Morrison, 'Dark patterns, the tricks websites use to make you say yes, explained' (1 April 2021) *Vox* <https://www.vox.com/recode/22351108/dark-patterns-ui-web-design-privacy> accessed 24 January 2022

[37] Bommasani, Rishi, et al. 'On the Opportunities and Risks of Foundation Models' (2021) arXiv preprint <https://arxiv.org/abs/2108.07258> accessed 10 January 2022

[38] For example, the training and use of FRT systems involves exposure to vast amounts of personal biometric data and the use of a smartwatch tracking your steps involves tracking your location

deployed through the use of additional 'smart' hardware such as live CCTVs, smart wearables, autonomous cars, smart home devices and voice assistants within our phones.

A. Internet of Things

The internet of things, popularly referred to as 'IoT', is a technology paradigm that enables communication between electronic devices and sensors through the Internet to facilitate human lives.[39] It relies on an interoperable network of devices that can communicate within their network while seamlessly processing one's personal data.[40] Examples of IoT include wearable watches that track heart rate, exercise parameters, and steps taken through sensors, or air purifiers that have embedded sensors to measure air quality. These smart devices can be connected through Bluetooth software with phones or computers to share the data gathered by their sensors. The boom in popularity enjoyed by smart home devices is evidenced in the use of voice recording, facial recognition and other kinds of pattern recognition and storage that lets personalised networks of devices function to an individual's preferences. On a larger scale, IoT is touted as the technology set to bring about the advent of smart cities with integrated surveillance, constant data processing, and a focus on safe and seamless experiences for all.[41]

B. Artificial Intelligence

AI applications require vast amounts of data in order to train, verify and reinforce desired outputs into its software. In this regard, higher data processing has led to increasingly refined models of AI in terms of learning and application.[42] Today's AI systems rely on deep neural networks and machine learning. These techniques teach the AI through computing a vast amount of data in an effort to increase its capability.[43]

In addition to the vast amount of data processing involved in training an AI model, there is also a far greater amount of personal data shared with the AI model upon deployment.[44] Countries across the world have commenced the use of AI powered facial recognition

[39] Sachin Kumar et al, 'Internet of Things is a revolutionary approach for future technology enhancement: a review' (2019) 6(111) Journal of Big Data <https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0268-2> accessed 19 January 2022
[40] Thomas Pasquier et al, 'Viewpoint- Personal Data and the Internet of Things' (2019) arXiv preprint <https://arxiv.org/pdf/1904.00156.pdf> accessed 19 January 2022
[41] Draft IoT Policy 2015, Ministry of Electronics and Information Technology
[42] Bommasani, Rishi, et al. 'On the Opportunities and Risks of Foundation Models' (2021) arXiv preprint <https://arxiv.org/abs/2108.07258> accessed 10 January 2022
[43] Ibid
[44] Pete Fussey, Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (July 2019) The Human Rights, Big Data and Technology Project <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/ 07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 29 January 2022

technology in law enforcement[45], increasing ease of access to public services[46] and health measures[47]. Additionally, certain countries have commenced projects that rely on AI to recommend decisions, as seen in the cases of computing risk assessments while sentencing an individual to prison[48] and immigration[49]. A major driving force behind emerging technology is the private sector, which has pioneered many of the emerging technologies that governments have started to adopt. Companies have commenced relying on AI-based tools for targeted advertising[50], algorithmic recommendations[51], voice assistants[52] and 'smart' home devices[53].

C. Impact on meaningful consent

The foregoing examples of emerging technologies offer a glimpse into tomorrow's 'new normal' of human interactions with technology. Keeping this in mind, it is worth considering the effect of emerging technologies on the ideal of informational privacy. The major issues with emerging technologies such as the Internet of Things and artificial intelligence deployment are (a) the ubiquitous processing of personal data, and (b) the lack of awareness on the extent of the data processing, as explained below:

(a) *Ubiquitous processing of personal data*

Once a smart home device is purchased, it becomes mandatory to consent to data processing to retain any use of that product. If one is forced to give up their personal data to use a product they own, is that consent meaningful? Let us assume that a user is notified through a privacy policy that their personal data shall be gathered while

[45] ANI, 'Madurai Police Launches Facial Recognition App To Reduce Crime Rate' (Tamil Nadu, 26 September 2020) *NDTV* <https://www.ndtv.com/tamil-nadu-news/madurai-police-launches-facial- recognition-app-facetagr-to-reduce-crime-rate-2301538> accessed 23 January 2022; HT Correspondent, 'Patiala Police nab 2 criminals using face recognition app' (Patiala, 1 June 2020) *Hindustan Times* <https://www.hindustantimes.com/chandigarh/patiala-police-nab-2-criminals -using-face-recognition-app/story-ZiGYD3Bh0GzUbSPls5S2JJ.html> accessed 23 January 2022

[46] KV Kurmanath, 'How Telangana government authenticates beneficiaries using AI, ML, Big Data and Deep Learning tools' (Hyderabad, November 2021) *The Hindu Business Line* <https://www.thehindubusinessline.com/info-tech/how-telangana-government-authenticates-beneficiaries-using-ai-ml-big-data-and-deep-learning-tools/article30025564.ece> accessed 23 January 2022

[47] Byron Kaye, 'Australia's two largest states trial facial recognition software to police pandemic rules' (17 September 2021) *Reuters* <https://www.reuters.com/world/asia-pacific/australias-two-largest-states-trial-facial-recognition-software-police-pandemic-2021-09-16/> accessed 16 January 2022

[48] Julia Angwin et al, 'Machine Bias' (23 May 2016) *ProPublica* <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 17 January 2022

[49] Petra Molnar, Lex Gill 'Bots at the gate: A human rights analysis of automated decision-making in Canada's immigration and refugee system' International Human Rights Program and the Citizen Lab (2018), available at <https://citizenlab.ca/wpcontent/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf> accessed 22 January 2022

[50] Ron Schmelzer, 'AI Makes A Splash In Advertising' (18 June 2020) *Forbes* <https://www.forbes.com/sites/cognitiveworld/2020/06/18/ai-makes-a-splash-in-advertising/?sh=6dcc7 9f47682> accessed 25 January 2022

[51] Kartik Hosanagar, 'Netflix, Tinder, Amazon all have automated algorithms. So, do humans have a choice anymore?' (12 May 2019) *The Print* <https://theprint.in/pageturner/excerpt/netflix-tinder-amazon-all-have-automated-algorithms-so-do-humans-have-a-choice-anymore/233261/> accessed 25 January 2022

[52] George Terzopoulos, Maya Satratzemi, 'Voice Assistants and Smart Speakers in Everyday Life and in Education' (2020) 19(3) Informatics in Education <https://files.eric.ed.gov/fulltext/EJ1267812.pdf> accessed 25 January 2022

[53] Ommid Saberi, Rebecca Menes, 'Artificial Intelligence and the Future for Smart Homes' (2020) EM Compass <https://www.ifc.org/wps/wcm/connect/6fc5b622-05cb-4ee9-b720-ab07591ac90e/EMCompass-Note-78-AI-Smart-Homes.pdf?MOD=AJPERES&CVID=n0S3dro> accessed 25 January 2022

using the device. Can the user question, request greater details, or negotiate for limiting the processing of personal data to what is necessary for the device's functions? The current framework of notice-and-consent does not consider these nuances. For example, websites that seek permission to collect data through cookies segregate cookies essential to the site's functionality, and non-essential cookies that help improve the website. A similar sliding scale where the consumer can set the level of personal data gathered from them, capable of being reaffirmed or altered at periodic intervals, may allow privacy-conscious users to negotiate over non-essential data processing.

Another aspect of IoT devices is the constant processing of data through various sensors. This processing is person-agnostic and to that extent is free from consent-based constraints.[54] A smart doorbell would process a visitor's face regardless of whether the visitor has consented to such processing.

AI deployment also raises issues with the notice-and-consent framework through its ubiquitous processing. The use of AI by the state on its citizens may not always be based on consent. Further, AI systems are being deployed by private companies for their product processes. A company providing certain services is legally free to deploy business strategies that involve targeted advertisements and algorithmic recommendations, provided this use is disclosed in its terms of use to solicit informed consent from users at the point of use. A user is then left with a binary, and in some cases meaningless, choice of either halting that service or continuing its use by consenting to AI features (as discussed above in the WhatsApp case). Even if the user gives such consent, they are unable to control the extent of profiling and targeted advertising they are subjected to, and the volume of their personal data points being processed to build an accurate profile.

(b) *lack of awareness on extent of personal data processed:*

IoT networks are compounded by their interactions with 'wearable' devices. These are devices that can be worn by users which track various biometric parameters, and give live updates to a user's doctor or record the data to be reviewed by the user later. Smart watches track a person's vitals and other associated information such as location, heart rates and logs of fitness metrics. Wearables face similar questions on the adequacy of notice-and-consent in light of their functionality depending on data processing and a user's limited scope of negotiation on the limits of data processing.

[54] Asher Gibson, 'The Internet Of Things and Privacy – Part Two: Solutions for Consent' (3 January 2020) Office of the Victorian Information Commissioner <https://ovic.vic.gov.au/blog/the-internet-of-things-and-privacy-part-two-solutions-for-consent/> accessed 28 January 2022

An individual's ability to give meaningful consent may be negated if an IoT-based smart city plans to require each individual to provide smart devices with some degree of personal data access. On a much smaller scale, a person's ability to give meaningful consent is negated if the person is unable to use a particular device they own unless they consent to also parting with their personal data.[55]

Emerging technological innovations in AI negate meaningful consent not only by denying users any meaningful control on how their data is processed, but also through opaque processes that hinder redressal. Developments in AI's computational models result in interpretable yet simple processes traded for accurate yet complex and unexplainable models for greater efficiency.[56] A negative profile built on certain data points may lead to harmful consequences such as higher rates of interest on loans[57], stringent sentencing norms[58] or creating a toxic environment for adolescent users of social media[59]. These damages are almost irreparable; consent revoked at this stage does not put the user back to their starting point as long as the data processor is entitled to retain the originally collected personal data.

The foregoing parts of this paper discussed the ways in which meaningful consent is undermined through the essential features of emerging technologies. The use of large-scale data processing raises questions on whether meaningful consent is enough to secure informational privacy. Further, the deployment of these emerging technologies by state agencies may operate outside the consent framework afforded to individuals. India currently deploys CCTVs at train stations and facial recognition technology as part of law enforcement norms.[60] These use cases are currently liable to be challenged on grounds of proportionality and necessity, relying on *Puttaswamy*.[61] However, in the context of a legislation mandating adoption of, and compliance with, an emerging technology, consent alone may not be effective in controlling state action and preserving informational privacy.

[55] Asher Gibson, 'The Internet Of Things and Privacy – Part One: Issues with Consent' (3 January 2020) Office of the Victorian Information Commissioner <https://ovic.vic.gov.au/blog/the-internet-of-things-and-privacy-part-one-issues-with-consent/> accessed 28 January 2022
[56] Bommasani, Rishi, et al. 'On the Opportunities and Risks of Foundation Models' (2021) arXiv preprint <https://arxiv.org/abs/2108.07258> accessed 10 January 2022
[57] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, pg. 9
[58] Karen Hao, 'AI is sending people to jail—and getting it wrong' (21 January 2019) MIT Technology Review <https://www.technologyreview.com/2019/01/21/137783/algorithms-criminal-justice-ai/> accessed 30 January 2022
[59] Georgia Wells et al, 'Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show' (14 September 2021) *The Wall Street Journal* <https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739> accessed 30 January 2022
[60] '500 facial recognition cameras deployed in Indian railway stations: Report' (27 August 2021) *Deccan Herald* <https://www.deccanherald.com/national/500-facial-recognition-cameras-deployed-in-indian-railway-stations-report-1024124.html> accessed 9 February 2022
[61] Justice KS Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1

III. Retaining informational privacy by pivoting to a regulatory approach

A. Regulatory approach to informational privacy

This paper does not dispute the importance given to consent-based privacy. Informational privacy can be understood to be a measure of *access control* and *use control*. An individual controls the levels of their personal data being processed, which reinforces their control and autonomy over their personal information and protects informational privacy. However, the standard notice-and-consent model itself may not sufficiently ensure informational privacy, as has been pointed out in Part 2. Instead, the practices underlying the notice-and-consent model determine the level of meaningful consent obtained from the data principal. Practices that complement the role of notice-and-consent are necessary to accommodate the privacy concerns raised by emerging technologies.

(a) *Consent as a continuous exercise:*

In *Distt. Registrar and Collector, Hyderabad v. Canara Bank*, the Supreme Court recognised the concept of privacy as relating to persons, and not places.[62] In other words, the right to informational privacy continues to apply even if it is outside the control of the individual. Reiterating this framing of informational privacy is essential to allow control over one's information even after consent has been given. However, data is intangible and non-rivalrous, and exercising control over one's data after permitting another entity to process it cannot merely be achieved through revoking that consent.[63]

(b) *Rights-based regulatory framework*

The continuous exercise of autonomy over one's data requires a holistic rights-based approach to data processing. A rights-based data processing regulation moves the exercise of consent from the moment of *collection* to the *duration of retention or use of the collected information*.[64] This reframing allows us to interact with our personal data even after we consent to let it be processed by another entity. It is necessary for these provisions to be legally enforceable.[65] Operating under an enforceable framework that grants rights to data principals and puts obligations on

[62] Distt. Registrar and Collector, Hyderabad v. Canara Bank, AIR 2005 SC 186
[63] Nestor Duch-Brown et al, 'The economics of ownership, access and trade in digital data' (2017) JRC Digital Economy Working Paper 2017-01 <https://ec.europa.eu/jrc/sites/default/files/jrc104756.pdf> accessed 30 January 2022
[64] FH Cate, Viktor Mayer-Schönberger, 'Notice and consent in a world of Big Data' (2013) 3(2) International Data Privacy Law <http://dx.doi.org/10.1093/idpl/ipt005> accessed 24 January 2022
[65] OECD Guidelines Governing The Protection Of Privacy And Transborder Flow Of Personal Data, 1980

data processors, thus, bridges the inadequacy of meaningful consent. This has been seen in efforts to move from a consent-based processing of personal data to a rights-based model of regulation in several jurisdictions.[66]

It should be pointed out that mere rights that empower data principals may not be sufficient to overcome the gaps to informational privacy. Emerging technologies make use of personal data in varied ways such as targeted advertising[67] and personalized feeds curated by algorithms designed to keep you on a website for as long as possible[68]. The exercise of rights requires corresponding obligations from data fiduciaries in order to be exercisable. Rights capable of being exercised by individuals is not a panacea to the problem. Rights-based obligations on data fiduciaries would require the exercise of a right by a data principal. Further, addressing the exercise of rights is necessarily a specific action, and does not affect the larger practices adopted by the data fiduciary as its default. Therefore, in addition to rights, a holistic approach to informational privacy requires the introduction of obligations on data fiduciaries. These may include obligations that permit the exercise of rights, and additional compliance measures that ensure a basic level of informational privacy is preserved. This is further discussed in Part 3 below.

B. Examining how emerging technology is likely to interact with the PDP Bill 2019

Part 2 discusses the issues raised by emerging technology in terms of meaningful consent and privacy. It is seen that ubiquitous processing of personal data and a lack of knowledge or control regarding the extent of personal data collected by emerging technologies undermine meaningful consent in preserving informational privacy. The foregoing section within Part 3 further discusses the need for a continuous interaction of the user with their personal data. Such an interaction permits users to exercise control over their data after it has been processed by another entity and offers greater autonomy, preserving informational privacy. This section shall examine these issues from the lens of the proposed PDP Bill 2019.

(a) Provisions in the PDP Bill that seek to supplement notice-and-consent

The PDP Bill 2019 was borne out of years of deliberations regarding India's approach to data protection and informational privacy. As noted by the Supreme Court, the Committee of Experts chaired by Justice (Retd.) BN Srikrishna presented

[66] General Data Protection Regulation, 2016
[67] David Morris, 'How marketers are increasingly using A.I. to persuade you to buy' (31 January 2020) *Fortune* <https://fortune.com/2020/01/31/ai-marketing-persuade/> accessed 1 February 2022
[68] Kartik Hosanagar, 'Netflix, Tinder, Amazon all have automated algorithms. So, do humans have a choice anymore?' (12 May 2019) *The Print* <https://theprint.in/pageturner/excerpt/netflix-tinder-amazon-all-have-automated-algorithms-so-do-humans-have-a-choice-anymore/233261/> accessed 25 January 2022

the report titled 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (the Srikrishna Report) which focussed on understanding informational privacy in a continuing sense. [69] The Srikrishna Report framed the idea of informational privacy as a continuous exercise of rights and obligations even after an individual has consented to their data being gathered.[70] The recommendations made by the Srikrishna Report were structured into a draft bill which was tabled before the Parliament as the Personal Data Protection Bill, 2019 (PDP Bill 2019).

The PDP Bill 2019 formulates a legal framework for personal data processing in India by setting out clear rights, obligations, legal norms and enforcement structures. These characteristics of the PDP Bill 2019 are central to a modern understanding of informational autonomy. The following provisions of the PDP Bill 2019 reflect the regulatory framework which offers greater control over data than merely notice-and-consent frameworks.

Meaningful consent continues to be a key facet of exercising autonomy over one's personal data. Accordingly, the standard notice-and-consent framework is recognised within the PDP Bill through a joint reading of Clauses 7 and 11. Clause 7 requires data fiduciaries to give data principals a notice at the time of collecting personal data. This notice must include the kind of data being collected, its purpose, basis, source, along with key information such as the right to withdraw consent and its procedure, third parties with whom this data may be shared, the data retention time and grievance redressal information. Similarly, Clause 11 imposes a positive obligation of consent prior to personal data processing, and requires the consent to be free, informed, specific, clear and revocable. Pertinently, provision of goods or services or performance of any contract cannot be made conditional on the data principal's consent to process personal data not essential for that performance.[71] Lastly, the PDP Bill 2019 introduces the concept of a 'consent manager' through whom a data principal may exercise their consent in an accessible and transparent manner.[72] Consent managers may be evolved as data fiduciaries that allow data principal to streamline and simplify consent granted to various data fiduciaries.[73] However, it remains to be seen whether consent managers are actually useful in simplifying consent for data principals and reducing 'consent fatigue'. Currently, the actual operations of consent managers are yet to be determined, based on regulations issued by the DPA.[74] The requirement of notice-and-consent thus

[69] 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (2018) Committee of Experts under the Chairmanship of Justice Srikrishna
[70] Chapter 5, ibid
[71] Clause 11(4), Personal Data Protection Bill, 2019
[72] Clause 23(3), Personal Data Protection Bill, 2019
[73] Samraat Basu, Siddharth Sonkar, 'Regulating Consent Managers in India: Towards Transparency and Trust in the Digital Economy' (1 April 2020) Oxford Business Law Blog <https://www.law.ox.ac.uk/business-law-blog/blog/2020/04/regulating-consent-managers-india-towards-transparency-and-trust> accessed 7 February 2022
[74] Clause 23(5), Personal Data Protection Bill, 2019

continues to be the standard method *at first instance* for exercising informational autonomy. However, the supplementary rights provided in the PDP Bill 2019 would enable data principals to continue exercising their informational autonomy in manners other than mere revocation of consent.

(b) *Rights framework supporting notice-and-consent under the PDP Bill 2019:*

Chapter V of the PDP Bill 2019, among others, sets out the following rights for data principals:

(i) The right to confirmation and access allows users to track who is processing their personal data and see a copy of the personal data processed.[75]

(ii) The right to correction and erasure further gives autonomy over processed personal data to the data principal, who may choose to correct inaccurate or outdated information, or may seek erasure of their collected information from any data fiduciary.[76]

(iii) Another facet of autonomy over personal data is a data principal's ability to transfer their data based on their interests, akin to the autonomy enjoyed over tangible property. The right to data portability allows users to receive a copy of all their personal data, including data generated through use of services or part of any profile on the data principal. The right to data portability further authorises data principals to have their personal data transferred by the current data fiduciary to any other data fiduciary.[77]

(iv) The right to be forgotten allows a data principal to seek a halt on continuing disclosure of personal data.[78] The right to be forgotten demonstrates the negative aspect of informational privacy, i.e., the right to be left alone, by empowering data principals to seek stoppage of any publication or disclosure of their personal data under certain circumstances. The need for this form of autonomy over one's data is seen in cases such as revenge pornography or wrongful accusations.[79]

The report on the PDP Bill by the Joint Parliamentary Committee (the JPC Report) has suggested an important addition to these rights. The JPC Report recognized the

[75] Clause 17, Personal Data Protection Bill, 2019
[76] Clause 18, Personal Data Protection Bill, 2019
[77] Clause 19(1)(b), Personal Data Protection Bill, 2019
[78] Clause 20, Personal Data Protection Bill, 2019
[79] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, C-131/12; Jorawer Singh Mundy v. Union of India, W.P.(C) 3918/2021

need for measures that can safeguard the privacy of a deceased data principal.[80] It recommends a right allowing data principals to nominate a legal heir or representative to exercise the right to be forgotten in the event of death of the data principal.[81] This is a positive recommendation, as it focuses on the data principal's post-mortem privacy rights and allows them to control their data upon their death.

The foregoing rights empower data principals through better knowledge of their data being processed, supplemented with the ability to alter, erase or transfer their personal data in the digital sphere. These rights come at a time when emerging technologies warrant data principals to have greater control over their personal data to retain informational autonomy. However, the exercise of rights by themselves is not an effective means to ensure informational privacy.

(c) *Regulatory obligations and structures supporting rights and autonomy:*

In addition to rights, the regulatory approach under the PDP Bill 2019 sets out obligations (and liabilities for failing to meet them) on data fiduciaries. These include basic concepts of data minimisation (minimal amount of personal data processing), by incorporating concepts of purpose limitation[82], collection limitation[83], and storage limitation[84]. Each data fiduciary is also required to meet the prescribed transparency and security standard norms. Importantly, each data fiduciary is required to set out a certified privacy-by-design policy.[85] Such a policy informs the activity of the data fiduciary by highlighting the importance given to informational privacy in its operational life cycle. Through such measures, the possible capabilities of emerging technology are tailored to the concerns of informational privacy.

These are baseline obligations applicable to all data fiduciaries. Certain data fiduciaries may also be classified as significant data fiduciaries.[86] This entails additional obligations such as requiring data protection impact assessments, appointment of a specialized data protection officer and conducting periodic audits on its policies and conduct.

Most importantly, the PDP Bill provides for a regulatory sandbox, in the interests of emerging technology. The regulatory sandbox is designed for emerging technology such as artificial intelligence, machine learning or other emerging technology products to be tested.[87] Participants in the sandbox are required to inform the Data

[80] Recommendation 39, Report of the Joint Committee on the Personal Data Protection Bill, 2019 (JPC Report)
[81] Ibid
[82] Clause 5, Personal Data Protection Bill, 2019
[83] Clause 6, Personal Data Protection Bill, 2019
[84] Clause 9, Personal Data Protection Bill, 2019
[85] Clause 22, Personal Data Protection Bill, 2019
[86] Clause 26, Personal Data Protection Bill, 2019
[87] Clause 40, Personal Data Protection Bill, 2019

Protection Authority regarding the innovative uses being tested, the data principals participating under the sandboxed project and the period for which it seeks to utilise the benefits of the sandbox. Similar sandboxes in the insurance sector and capital markets sector have received numerous applications.[88]

(d) *Enforcing regulatory measures and remedies:*

The PDP Bill 2019 also provides for an enforcement structure that actualises the rights and obligations for all stakeholders. The PDP Bill 2019 sets out a regulatory structure headed by a data protection authority (DPA) responsible for framing regulations[89], enforcing obligations through reporting requirements[90], conducting inquiries[91] and levying penalties[92]. For example, data fiduciaries that cater to a certain threshold of the population are required to undertake periodic audits on their data processing operations.[93] Further, they are required to appoint data protection officers for carrying out the obligations of the PDP Bill 2019.[94] Importantly, significant data fiduciaries are required to conduct a data protection impact assessment before undertaking any processing of sensitive personal data or profiling through emerging technologies.[95]

Additionally, the PDP Bill 2019 sets out monetary consequences for data fiduciaries or processors that fail in adhering to its provisions. Failure to comply with processing obligations for child personal data may attract a fixed penalty or a penalty based on worldwide turnover.[96] Similarly, penalties for non-reporting of data breaches or register as significant data fiduciaries attract monetary penalties.[97] The PDP Bill 2019 recognises that personal data can be converted through an anonymization process, and prescribes criminal sanctions for attempts to re-identify anonymised data.[98]

IV. Exemptions granted by the PDP Bill 2019

The holistic regulatory approach promised by the PDP Bill 2019 is undercut by certain provisions that allow sweeping exemptions to the central government.[99] While the PDP Bill 2019 exempts various categories of data processing for specified purposes, clause 35 suffers from a lack of sufficient safeguards. The current version of the PDP Bill 2019 only

[88] Insurance Regulatory and Development Authority of India, '3rd tranche of approvals under the Regulatory Sandbox' (3 June 2020) <https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx ?page=PageNo4142&flag=1> accessed 4 February 2022; Joel Rebello, 'RBI's fourth regulatory sandbox cohort on financial frauds' (8 October 2021) *The Economic Times* <https://economictimes.indiatimes.com/news/economy/policy/rbis-fourth-regulatory-sandbox-cohort-on-financial-frauds/articleshow/86859943.cms> accessed 4 February 2022
[89] Clause 94, Personal Data Protection Bill, 2019
[90] Clauses 25(6), 29, Personal Data Protection Bill, 2019
[91] Clauses 52-54, Personal Data Protection Bill, 2019
[92] Clauses 57-62, 64, Personal Data Protection Bill, 2019
[93] Clause 29, Personal Data Protection Bill, 2019
[94] Clause 30, Personal Data Protection Bill, 2019
[95] Clause 27, Personal Data Protection Bill, 2019
[96] Clause 57(2), Personal Data Protection Bill, 2019
[97] Clause 57(1), Personal Data Protection Bill, 2019
[98] Clause 83, Personal Data Protection Bill, 2019
[99] Clause 35, Personal Data Protection Bill, 2019

requires the reasons to be recorded in writing, upon which the central government may exempt any agency from any or all parts of this law.[100] In this regard, the JPC Report has proposed a welcome addition to clause 35 by requiring the alternative procedures followed by the exempted agency to be just, fair, reasonable and proportionate in nature.[101]

The scope of these potential exemptions raises concerns, particularly in light of the deployment of various emerging technology solutions by the central government in recent years. The applications of AI and IoT only by the central government include the programs listed below. In addition to these, there are at least seventy-five instances where emerging technology has been deployed within India, with at least nineteen projects being launched by the central and state governments.[102]

S. No.	Ministry	Type of emerging technology	Name of project	Purpose
1.	Ministry of Civil Aviation	Facial recognition technology (FRT)	Digiyatra[103]	Authentication: increasing ease of access to airports
2.	UIDAI, Ministry of Electronics and Information Technology (MEITY)	FRT	Authentication Based Facial Recognition[104]	Authentication: ease of authentication for Aadhar card
3.	UIDAI, MEITY	FRT	Authentication Based Facial Recognition[105]	Authentication- biometric authentication of Covid-19 vaccine recipients

[100] Ibid
[101] Recommendation 56, JPC Report
[102] '75@75: India's AI Journey' (2021) Ministry of Electronics and Information Technology <https://www.meity.gov.in/writereaddata/files/75-75-India-AI-Journey.pdf> accessed 3 February 2022
[103] '"Digi Yatra" Reimagining Air Travel in India' (2018) Ministry of
[104] Newsdesk, 'UIDAI introducing facial recognition for Aadhaar authentication will ensure greater inclusion' (New Delhi, 25 August 2018) *Financial Express* <https://www.financialexpress.com/opinion/uidai-introducing-facial-recognition-for-aadhaar-authentication-will-ensure-greater-inclusion/1291516/> accessed 3 February 2022
[105] India Today Tech, 'Aadhaar face recognition could be made mandatory for COVID vaccination, pilot testing is on' (New Delhi, 9 April 2021) *India Today* <https://www.indiatoday.in/technology/news/story/aadhaar-face-recognition-could-be-made-mandatory-for-covid-vaccination-pilot-testing-is-on-1789024-2021-04-09> accessed 3 February 2022

4.	Central Board for Secondary Education	FRT	Face Matching Technology[106]	Educational- Identity authentication to access academic documents
5.	MEITY	Conversational AI chatbot	Intelligent Virtual Assistant[107]	Used in the MyGov Corona Helpdesk to interact with citizens having doubts
6.	Jal Shakti Ministry	Internet of Things	Unnamed[108]	Used in monitoring implementation of Jal Jeevan Mission
7.	NHAI, Ministry of Road Transport and Highways of India	Location tracking AI	Attendance Monitoring System[109]	Real-time tracking of employees to ensure attendance

The increased deployment of these emerging technologies by the central government raises concerns over the exemptions provided within the PDP Bill 2019. As can be seen above, the foregoing AI-based programs involve processing of personal data as part of their functioning. Additionally, these provisions create an incentive for agencies to claim broad exemptions for a future purpose, with central government agencies such as the UIDAI[110] and the Income Tax Department[111] already claiming exemptions prior to the bill being finalized. An individual having no awareness of the safeguards enjoyed by their personal data in an exempted agency does not retain means to ensure informational privacy. Even if an agency receives full exemption from the law, the wisdom or benefit of these exemptions for obligations such as reporting data breaches or maintaining security standards is not clear at this stage.

[106] Director IT & Projects 'Availability of Digital Academic Documents using "Face Matching Technology"' Central Board of Secondary Education <https://www.cbse.gov.in/cbsenew/documents/Face%20Matching%20Technology.pdf> accessed 3 February 2022
[107] IANS, 'India's AI enabled MyGov Corona Helpdesk wins two global awards' (30 June 2020) *Business Insider India* <https://www.businessinsider.in/tech/news/indias-ai-enabled-mygov-corona-helpdesk-wins-two-global-awards/articleshow/76717104.cms> accessed 3 February 2022
[108] PIB Delhi, 'Jal Jeevan Mission deploys first-of-its-kind sensor-based IoT devices to monitor rural drinking water supply systems' (31 March 2021) Ministry of Jal Shakti <https://pib.gov.in/PressReleasePage.aspx?PRID=1708701#:~:text=To%20monitor%20the%20rural%20drinking,more%20than%20six%20lakh%20villages> accessed 3 February 2022
[109] PTI, 'NHAI introduces AI-based face recognition system for attendance monitoring' (5 March 2021) *The Economic Times* <https://economictimes.indiatimes.com/news/economy/infrastructure/nhai-introduces-ai-based-face-recognition-system-for-attendance-monitoring/articleshow/81351409.cms ?from=mdr> accessed 3 February 2022
[110] Sobhana Nair, 'UIDAI wants exemption from Data Protection Bill' (29 October 2021) *The Hindu* <https://www.thehindu.com/news/national/uidai-wants-exemption-from-data-protection-bill/article37238680.ece> accessed 3 February 2022
[111] Deeksha Bhardwaj, 'Karnataka, UIDAI, I-T dept flag concerns over Personal Data Protection Bill' (30 October 2021) *Hindustan Times* <https://www.hindustantimes.com/india-news/karnataka-uidai-i-t-dept-flag-concerns-over-personal-data-protection-bill-101635533754592.html> accessed 3 February 2022

Conclusion

This paper has sought to examine the idea of informational privacy, protected under the Constitution, from the lens of meaningful consent. The right to choose with whom an individual may share their data is a facet of the right to privacy, and forms the principle of informational autonomy. Exercising meaningful consent to allow personal data processing may be viewed either as an economic choice by a rational consumer or as a human dignity-based choice that preserves informational privacy. Notice-and-consent has been the prominent traditional model to allow individuals to provide meaningful consent by exercising their informational autonomy.

However, the rise in the use of AI systems and IoT devices that include smart devices and wearable technology raises concerns over the meaningful consent aspect of informational privacy. Ubiquitous data processing and lack of awareness of the extent of data processed raise concerns of informational privacy that consent itself cannot resolve. The need of the hour, thus, is a regulatory approach that enhances informational privacy by presenting data principals with rights that supplement their meaningful consent, and imposes baseline obligations on data fiduciaries involved in these processes.

The PDP Bill 2019 aims to provide a holistic regulatory framework from that lens. It allows for greater informational privacy through a framework of exercisable rights and enforceable obligations. Further, it sets out basic measures of limitation, transparency, accountability and security to be followed by data fiduciaries. These provisions frame the preservation of informational privacy as a duty towards the state at large, and not just actions taken in response to individual exercise of rights. In addition to the rights and obligations, the PDP Bill also takes cognizance of the unique regulatory challenges posed by emerging technologies and has provided for a sandboxing regime to be implemented. Certain recommendations of the recently released JPC Report, with reference to post-mortem privacy and safeguards to be followed by exempted agencies, are positive in nature. The final form of this law, along with rules and regulations formed to carry out its goals, is awaited to see the true strength of this law in preserving informational privacy.

www.vidhilegalpolicy.in
Vidhi Centre for Legal Policy
A-232, Ratan Lal Sahdev Marg,
Block A, Defence Colony
New Delhi 110024
011-43102767/43831699
vclp@vidhilegalpolicy.in