
THE PRIVACY PARADOX AND THE ILLUSION OF CONTROL: A CRITICAL STUDY OF DIGITAL PRIVACY IN INDIA

Priyadarshini Chakraborty, Manipal Law School, Bengaluru

ABSTRACT

The fast changing and rapid expansion of the digital economy in India has not only transformed the way personal data is collected, processed, and utilised but also has transformed how people value their own personal data these days. At the very core end of this transformation lies the concept of consent which forms a legal basis of processing data under the Digital Personal Data Protection Act, 2023. With the current enforcement and more awareness of protection of personal data individuals worry a lot about their privacy, apart from all the privacy awareness still individuals go ahead and share all sorts of personal stuff online without much thought. This whole concept is known as the privacy paradox. It makes individuals really think of the fact of how the usual consent setups let them have real control over their own data. This paper will study the concept of privacy paradox from the viewpoint of behavioural, technological, and legal dimensions within the Indian context. It will further argue the structural issues such as information asymmetry, cognitive overload and interface manipulation which undermines the validity of current consent mechanism. The paper further discusses the Indian data protection regime which is still progressing in its principle remains limited in addressing deeper concerns. A conclusion will be drawn by advocating a shift from a formal consent autonomy through stronger regulatory interventions and a design-based protections.

Keywords: Privacy paradox, data protection, Digital Personal Data Protection Act, 2023, Consent, Privacy.

Research Question

1. Do users understand the reality of protecting privacy as well as protection of personal data?
2. Do users value their protection of personal data in reality?
3. How much effect does the concept of privacy paradox affects the protection of personal data of individuals?

Research Problem

The concept of the Indian data framework is fundamentally built on the idea that individuals will exercise their personal data control through consent which is informed. However, in reality individuals disclose their own personal data despite expressing their strong privacy concerns. This contradiction is known as the privacy paradox, and it signs towards a gap between legal assumptions and actual user behaviour. The main problem lies in the fact that whether consent, which is currently exercised as structured, can truly be considered as “informed” and “free” in such an environment which is characterised by complex privacy policies, manipulative interface design, and unequal bargaining power between users and platforms.

Research Methodology

This paper will adopt a doctrinal methodology to understand the concept of privacy paradox in the Indian legal and digital sphere.

Introduction

The massive digital revolution in India has marked a huge exponential growth in the penetration of internet, using of smartphones and platform-based services. Personal data has become an asset of modern economies by playing a pivotal role, from e-commerce to digital payments and social media. In response to such growing concerns about the misuse of personal data of individuals India enacted the Digital Personal Data Protection Act, 2023.

The Act seeks to regulate the processing of personal data and ensure individual digital privacy. One of the most essential points that is more elaborated upon is the concept of consent in this regulatory framework.

The individuals recognised as the “Data Principals” here are expected to make informed decisions regarding the use of their own data. Such an assumption is really being challenged by a phenomenon known as the privacy paradox. In most of the times users understand and claim to value their privacy highly but their behaviour reflects a willingness to disclose personal information in exchange for convenience, access, or perceived benefits offered by the platforms. This leaves with a critical question about the effectiveness of consent mechanism as a legal tool. “Can consent be truly considered meaningful in cases where users fail to act in accordance with their stated preferences?” This paper will explore this question in the Indian context by examining how behavioural realities intersect with the legal frameworks.

Understanding the concept of Privacy Paradox

The concept of privacy paradox can be referred to as inconsistency between individuals’ privacy attitudes and their actual behaviour of sharing of data.¹ While users express their concerns regarding surveillance, data breaches, and misuse of their own personal information still they frequently engage in practices that compromise their privacy. Such as accepting terms and conditions without reading them once or granting excessive permissions to mobile applications. Traditional economic theories explain such a kind of behaviour as a rational trade-off between privacy and utility.² Users may knowingly sacrifice their own privacy for convenience or access to services. All such explanations are insufficient. Behavioural studies suggest and point out that users operate under conditions of bounded rationality, where decision-making is influenced by cognitive limitations, heuristics, and biases.

For example, most of the times users underestimate long term risks while trading with immediate benefits. It is also a fact that the complex, long privacy policies make it impractical for users to fully understand the implications of their consent.³ Due to such reasons also the privacy paradox is not merely a matter of choice but a reflection of systemic constraints on informed decision-making.⁴

¹ Spyros Kokolakis, *Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon*, 64 *Computers & Security* 122 (2017)

² Susanne Barth & Menno D. T. de Jong, *The Privacy Paradox—Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior: A Systematic Literature Review*, 34 *Telematics & Informatics* 1038 (2017)

³ Nina Gerber, Paul Gerber & Melanie Volkamer, *Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior*, 38 *Computers & Security* 226 (2018).

⁴ Karlsruhe Institute of Technology (SECUSO), *Privacy Paradox – Theories and Models*

The Indian Digital Ecosystem and Data Practices

India's digital ecosystem presents a unique and a rare characteristic which further intensifies the privacy paradox. The rapid adoption of digital services, driven by the affordability and core government initiatives like that of "Digital India" has brought millions of first-time users online and onboarded to the digital world. Sadly, most of these users lack digital literacy, making them particularly more vulnerable to exploitative data practices.

Digital platforms most of the time collect extensive personal data like location, browsing behaviour, financial information and even biometric data.⁵ Maximum of the time privacy policies are typically drafted in a very complex legal language which is inaccessible to the average user. Furthermore, consent mechanisms are specifically designed to prioritise speed and convenience often encouraging users to accept terms without any scrutiny.⁶

The widespread use of "take-it-or-leave-it" contracts further escalate problems. Most of the users have little bargaining power and most of the times are compelled to accept terms to access essential services. This raises concerns about whether consent in such scenarios can truly be considered voluntary.

Consent under DPDP Act, 2023

Consent plays a crucial role in data processing under the DPDP Act, 2023.⁷ For instance, consent should be free, informed, specific, and unambiguous. On its face value, the Act shows a great sense of commitment to ensuring user autonomy. Nevertheless, the effectiveness of such provisions is contingent on their practical application. As shown by the privacy paradox, there are many obstacles associated with them:

- Informed Consent: Users do not go through privacy policies of most platforms since they are lengthy and too complicated.
- Free Consent: Users cannot say 'no' to certain terms since there are no alternatives to

⁵ H. Jeff Smith, Tamara Dinev & Heng Xu, *Information Privacy Research: An Interdisciplinary Review*, 35 MIS Quarterly 989 (2011).

⁶ Tamara Dinev & Paul Hart, *An Extended Privacy Calculus Model for E-Commerce Transactions*, 17 Information Systems Research 61 (2006).

⁷ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023, § 6 (India).

those services.

- Specific Consent: Data collected by companies in question is rather vague.
- Unambiguous Consent: Various techniques used in designing interface of applications might interfere with the process.

As can be seen, the Act creates a good legal framework. However, it does not address some other issues related to the privacy paradox.

5. Dark Patterns and Design Issues

One of the critical reasons behind the privacy paradox phenomenon is the implementation of so called “dark patterns,” i.e. techniques used by companies to manipulate their customers’ behaviour.⁸ They include:

- Prevalent settings that promote data exchange
- Complicated ways to reject a request for data
- Highlighting the acceptance option visually
- Distorted wording used to conceal possible consequences

The implementation of such techniques exploits various cognitive biases and makes it unlikely for people to make decisions aimed at protecting their privacy.⁹ Considering the diversity of digital skills within India, this issue becomes even more evident. The existence of dark patterns leads to several legal considerations.¹⁰ What is the validity of the consent that was granted under manipulative circumstances?

6. The concept of user autonomy needs revaluation with respect to data protection

Since the concept of consent is limited, it becomes necessary to develop a more substantial

⁸ Ioannis Paspatis, Aggeliki Tsohou & Spyros Kokolakis, *How Is Privacy Behavior Formulated? A Review of Current Research and Synthesis of Information Privacy Behavioral Factors*, 7 *Multimodal Tech. & Interaction* 76 (2023).

⁹ Spyros Kokolakis, *Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon*, 64 *Computers & Security* 122 (2017).

¹⁰ Meredydd Williams, Jason R. C. Nurse & Sadie Creese, *The Perfect Storm: The Privacy Paradox and the Internet-of-Things*, *IEEE Internet of Things Journal* (2016).

concept of autonomy which would consider structural inequality and behavioural obstacles.

They include the following:

- Privacy By Design: Designing digital technology with an inherent level of privacy protection through minimum data use and security measures.
- Regulation of Dark Patterns: Banning the use of manipulative design in interfaces to avoid misinformed consent of users.
- Standardization of Notice Forms: Creating standardized notice formats for better user protection.
- Greater Accountability: Requiring data fiduciaries to be held accountable for their data policies and use.

This approach places emphasis on structural solutions, acknowledging that user autonomy can only occur when there are structural safeguards in place.

7. Conclusion

The privacy paradox reveals an inherent weakness within the existing framework of data protection, the excessive dependence upon consent as the main instrument of protecting individuals' privacy.¹¹ The situation in India becomes even more challenging due to the existence of digital illiteracy, bargaining inequality, and manipulation practices among developers of various software applications.

Even though the DPDPA, 2023 has marked a positive move toward improving data security, the law needs to adapt to the reality of modern users' practices. Consent alone cannot be effective in controlling personal data.

The development of new standards of data protection involves transcending the formal conception of consent and focusing on substantive autonomy and accountability.¹²

¹¹ *Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms*, Cambridge University Press (Oct. 28, 2019).

¹² Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, 3 IEEE Security & Privacy 26 (2005).