# THE PARADOX OF CHOICE: DIGITAL CONSENT AND CONSUMER VULNERABILITY IN INDIA

Drashya Sharma, National Law University Meghalaya

Kaushik Kr Singh, National Law University Meghalaya

## ABSTRACT

The meteoric rise in digitalization has changed how consumer consent is given and obtained; this evolution has sparked new issues regarding consumer autonomy and the reliability of digital contracts. This article analyses the issue of the choice paradox in the digital marketplace of India and particularly looks at whether a mere click on the "I Agree" button is sufficient to grant consent. Moreover, it will examine the current legal situation in India based on its various acts, such as the Indian Contract Act, 1872, the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, and the Consumer Protection Act, 2019.

Furthermore, the article examines how consumer choices get influenced by deceptive interfaces and personalized algorithms, especially when consumers lack digital literacy. The article focuses on the problem that, prima facie, consumers are provided with multiple options, but consumers may not be acting autonomously in reality, as interfaces may manipulate decisions in various ways. Ultimately, the article envisions a path towards meaningful, informed, and expressed consent and a better marketplace wherein consumers and service providers coexist in a balanced ecosystem.

## Introduction

In the traditional contract law, consent formed the basis of legal obligations. Under Indian contract law, the formation of a contract requires consent between the parties, while the principle of free consent addresses the circumstances under which consent is given[1]. However, as the world transitions to digitalisation, the way consent is obtained has changed. Today, consumers routinely encounter clickwrap agreements containing terms and conditions that are usually set by the platforms; these are a form of standard contract with no scope for negotiation, and consumers usually agree to the conditions with the click of a button. What was intended to be an expression of choice, however, raises concerns about whether the mere click of a button constitutes a meaningful exercise of consent.

This tension between the established legal principles and the realities of the digital environment is further intensified by manipulative interface designs, dark patterns and algorithmic personalisation. Digital vulnerability and information asymmetry can leave consumers susceptible to practices that influence their decisions without their full understanding. Complex terminology, lengthy disclosures, and interface designs that steer consumers toward platform-preferred outcomes further raise questions about the extent to which consumer can exercise their choices independently[2].

In light of these concerns, this article examines the legal validity of such agreements in India. Furthermore, it looks into how consumers' digital vulnerability and how design interfaces can manufacture consent, how practices such as algorithmic personification may affect consumer autonomy and free choice, and the reforms necessary to move towards meaningful and genuine consent.

## Legal Framework Governing Digital Consent

In the Indian legal context, consent carries profound legal weight, especially in traditional contracts. The advancement of technology and various social media platforms has turned the traditional consent into a clickwrap agreement.[3] On online platforms, users are typically presented with a pre-ticked dialogue box outlining the platform's terms and conditions, which

[1] Indian Contract Act, No. 9 of 1872, §§ 10, 13–14 (India).
[2] Guidelines for Prevention and Regulation of Dark Patterns, 2023, Gazette of India, Extraordinary, pt. III, sec. 4 (Nov. 30, 2023).
[3] Information Technology Act, 2000, No. 21 of 2000, § 10A (India)

may prevent them from accessing the application unless they ratify the conditions. In many cases, the systems on these platforms are designed to continuously prompt users with dialogue boxes until they agree to the terms.

These circumstances highlight the need to critically examine the legal validity of such agreements.

**Indian Contract Act, 1872**: The Act establishes the essential elements of a contract. Under section 13 of the Indian Contract Act, consent is valid when there exists a meeting of minds between the individuals, while section 14 subsequently highlights the need for free consent.[4]

In the digital age, contracts are standard-form, with terms and conditions that are generally non-negotiable and set by the platforms. The users are usually presented with a dialogue box containing terms and conditions, in which they are deprived of the right to alter the terms, thereby leaving them with no real bargaining power. This directly calls into question the consent obtained through this method and whether such consent is actually free as per section 14 and in congruence with it.

Manipulative interface designs, such as nagging in pop-ups or coercive prompts, may, at the same time, affect the application's operation, which may subsequently undermine section 14 of the contract, as these interfaces may alter the user experience and encourage the user to agree to the conditions.[5]

Additionally, the Contract Act explicitly mentions that the user should be informed of consent, meaning the user should be aware of all the terms and risks involved; however, clickwrap agreements are often accompanied by fancy text and excessive jargon, which often prevents the user from understanding the terms of the platform, thereby undermining the genuine and informed consent of the user.

**Digital Personal Data Protection Act, 2023-**The DPDP Act states that consent must be specific, informed, unconditional and most importantly**,** unambiguous.[6] However, platforms often refrain from explaining the rationale for seeking user permissions. Even when platforms

[4] Indian Contract Act, 1872, No. 9 of 1872, §§ 10, 13–14 (India).
[5] Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns, 2023, cl. 2(1)(e), Annexure I (Nov. 30, 2023).
[6] Digital Personal Data Protection Act, No. 22 of 2023, § 6(1), India Code (India).

provide justifications, they lack clarity and offer few concrete details. Furthermore, Section 5 of the act requires platforms to notify users before collecting and subsequently using their data, yet in practice, the depth of information provided by platforms varies.[7]

Section 12 gives consumers the right to erasure.[8] The user may request that an app completely delete their personal data once they stop using the service. Still, in many cases, the platform's data deletion procedure is either unavailable or its architecture is so complex that it hinders access to the feature.

**Information Technology Act, 2000 –** The IT Act of 2000 is the primary law in India that governs cybersecurity. This act plays a foundational role as Section 10A of the IT Act legalises contracts formed through digital communications, website clicks (clickwrap agreements), and email confirmations.[9] Nevertheless, section 43 of the same act mandates penalties and compensation of up to Rs. 1 crore if a business or a hacker damages, copies, or extracts consumer data[10] without authorisation. The fundamental question is whether consumers actually authorise the subsequent use of their data for commercial purposes, and whether a mere tap on "I Agree" by the user amounts to genuine consent.

**Consumer Protection Act, 2019 –** The Consumer Protection Act, 2019, is a consumer-friendly framework which addresses consumer rights. It includes provisions addressing contemporary challenges, with a special emphasis on the digital ecosystem and recent needs.

Section 2 (46) of the statute defines an unfair contract as any agreement that imposes unreasonable conditions or harms consumer rights[11]. It has frequently been observed that certain platforms ask consumers for permissions under the guise of enabling app functionality, even though those permissions may be unrelated to the platform's actual purpose and usage. For example, a QR scanning application may require permission to "access all the media" available on the device. Platforms, as per their usage requirements, may request permissions to access "media or gallery"; however, demanding access to all media is unreasonable. Furthermore, denying such permissions prevents the user from accessing the application

[7] Id. § 5.
[8] Digital Personal Data Protection Act, No. 22 of 2023, § 12, India Code (India).
[9] Information Technology Act, No. 21 of 2000, § 10A, India Code (India).
[10] Id. § 43.
[11] Consumer Protection Act, No. 35 of 2019, § 2(46), India Code (India).

completely.

The act serves as a protection mechanism to prevent consumers from being deceived; however, such digital platforms may undermine the spirit of the consumer framework.[12]

**When Consent is Designed: The Influence of Dark Patterns**

Dark patterns are user interfaces or digital design choices deliberately crafted to trick, deceive, or manipulate online users into making decisions that benefit a business at that user's expense.[13] These interface designs subvert users' free consent by manoeuvring them into consenting through engineered systems. E-commerce and social media platforms have generally exploited behavioural psychology to their advantage, effectively using cognitive biases as a weapon.[14]

Some of the common deceptive design interfaces used by the platforms include[15] –

**Basket sneaking** occurs when a platform secretly adds an extra paid item or service to the shopping cart without the consumer's explicit consent.[16] Users are generally in a hurry and sometimes overlook details, and the platform uses this to its advantage, generating extra profit.

**Confirm shamming** – this way uses emotional manipulation, guilt, or fear to pressure the consumers into choosing an option that the user would otherwise decline.[17] They psychologically trick users by using phrases that subtly force them to click the accept button rather than the decline button. For instance, the decline button, instead of being neutral-"No, I don't want"-may include a phrase that says, "No, I prefer not to get any benefit."

**False urgency** – humans often experience FOMO (fear of missing out), and many platforms exploit it by creating a false sense of urgency.[18] For instance, the platform may state that the new dress will be sold out because only 2 pieces are left, which may not be true. Still, this way

[12] Consumer Protection Act, No. 35 of 2019, §§ 2(47), 18; Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns, 2023 (Nov. 30, 2023).
[13] Jamie Luguri & Lior Jacob Strahilevitz, Shining a Light on Dark Patterns, 13 J. Legal Analysis 43, 43–109 (2021).
[14] Arunesh Mathur et al., Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites, 3 Proc. ACM on Hum.-Comput. Interaction, no. CSCW, art. 81, at 1–32 (2019).
[15] Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns, 2023, Annexure I (Nov. 30, 2023).
[16] Guidelines for Prevention and Regulation of Dark Patterns, supra note 2, Annexure I (defining "Basket Sneaking").
[17] Id. (defining "Confirm Shaming").
[18] Id. (defining "False Urgency").

the consumer would, despite being reluctant, buy it as they would believe that if I think, then I might lose the chance to buy the dress, and hence they don't let the consumer think or make an effective choice.

Eventually, digital platforms use dark patterns to ensure that consumers' choices align with the platform's objectives, using numerous behavioural psychology and deceptive design techniques. Consumers remain under the belief that they have actively consented, but the platforms shape their consent through the interface.[19]

**Consent amid vulnerability and information asymmetry**

In the contemporary age, digitalisation has transformed the way consumers interact with the market. From instant purchases on delivery apps to large-scale business operations, digital technologies have shaped consumer behaviour. Furthermore, consumers today have an abundance of choices, often just a single click away on their devices. However, the availability of choices does not guarantee genuine access to exercise them.

Digital literacy acts as a link between consumers' on-screen choices and the legal concept of consent; in simpler terms, it is a bridge between consumers and platforms, enabling them to understand and exercise the choices presented to them.

In India, a significant portion of the population lives in rural areas and remains agrarian, which is why digital literacy remains disproportionately low.[20] This digital literacy deficit makes Indians more vulnerable to digital platforms.[21] The vulnerability arises from platforms' ability to leverage consumer ignorance and exploit these users for their own benefit. Platforms usually capitalise on this ignorance to obtain consent and influence outcomes. For instance, platforms usually present everything in officialese, which is difficult for the general public to understand; furthermore, the terms and conditions required by the platforms are often presented in languages other than the local language, which makes them even more difficult to comprehend.[22] This digital vulnerability creates information asymmetry between consumers

[19] Jamie Luguri & Lior Jacob Strahilevitz, supra note 13, at 43–46.
[20] Ministry of Statistics and Programme Implementation, Government of India, Household Consumption Expenditure Survey: 2023–24 (2025); Ministry of Statistics and Programme Implementation, Government of India, Multiple Indicator Survey in India, 2020–21 (2023).
[21] Telecom Regulatory Authority of India, Digital Literacy and Digital Skills in India 79 (Sept. 14, 2023).
[22] Adeeth Cariappa et al., The Digital Landscape in Eastern India: Findings from the Digital Needs Assessment Surveys from Bihar and Odisha, India (Int'l Food Pol'y Rsch. Inst. 2024).

and digital platforms, further exacerbating the power imbalance between them.

Amartya Sen's entitlement theory further states that starvation is caused not by a lack of availability but by a lack of means to access them.[23] Applying this theory, if people lack digital literacy, it would be difficult for them to access the available choices on digital platforms.

This information asymmetry and power imbalance manifest in various forms, such as non-negotiable platform requests that users consent to in everyday platform interactions because they rarely have an alternative. The users accept these conditions not genuinely, but because they do not understand the legal gravity of what they are signing away. This proves that digital consent in this ecosystem has become merely a mechanical gesture, lacking a genuine, meaningful choice.

**The Illusion of choice: Is digital consent truly voluntary?**

In the legal context, consumer choice is often reduced to the mere availability of options on the screen. However, it is important to distinguish between the availability of options and a truly meaningful choice. A meaningful choice is one in which the person has equal access to all available alternatives, no option is excluded, and the consumer has an equal chance to weigh them without manipulation or bias.

At its core, the Contract Act states that a contract or agreement between two individuals occurs when there is consensus ad idem, or a meeting of minds; however, this threshold is often not met when digital platforms engineer their systems to curate an environment that generates their desired outcome.[24] These platforms often remove the voluntariness that contract law demands.

In today's digital market, this legal standard is repeatedly breached through manipulative designs. For instance, many platforms display cookie consent banners in bright colours; however, the "reject cookies" option is usually hidden behind multi-step processes.[25] Similarly, this pattern is observed in search results when a specific brand is searched, but sponsored results appear throughout the platform, affecting consumers' decisions. Not just this; the same pattern can be observed when certain social media apps make it very easy for users to create an account,

[23] Amartya Sen, Poverty and Famines: An Essay on Entitlement and Deprivation (Clarendon Press 1981).
[24] Indian Contract Act, No. 9 of 1872, § 13 (India).
[25] Cristiana Firullo, Francesco Decarolis & Cristobal Cheyre, Consent and Choice: Experimental Evidence on User Behavior at Consent Banners, CEPR Discussion Paper No. 22078 (2026)

but a very difficult, layered process to actually delete it.[26]

In light of these structural realities, the question of whether consumer autonomy actually exists is debated. At the same time, digital platforms present an illusion of multiple choices and a consumer-based economy, consent is often structured and extracted from consumers in various ways. Ultimately, consumer autonomy seems limited, and the scope of genuine consent is even narrower.

**When personalization goes beyond consent**

Algorithmic personalisation is a system through which platforms access user data and later utilise it to personalise user content, effectively catering to the needs and preferences of the user behind the screen. A clear manifestation of this process may be social media platforms effectively collecting user data, such as their search history or watch time, to personalise content for them, or ecommerce platforms collecting data to advertise products consumers would actually buy.[27]

At first glance, this might seem like a beneficial practice, as it may enhance the consumer experience and allow them to see things they genuinely like, rather than being shown unnecessary items. Furthermore, this is a commercially lucrative process for social media platforms, as it can substantially increase user watch time, which is profitable for them.[28] For e-commerce platforms, this system could drive better sales by understanding consumer needs and by running advertisements using personalisation. However, this model reveals several structural complications in execution, such as –

**Disguised surveillance** – Digital surveillance refers to the continuous online tracking of a person's online behaviour, location, choices and habits by platforms. While platforms routinely justify collecting data under the banner of personalisation and enhancing the user experience, this may pose serious risks to privacy, as the same algorithmic personalisation mechanism can easily be double-used as a tool for digital surveillance. Users consent to personalisation in exchange for a more tailored user experience, but platforms also collect location-related data

[26] Sebastian C. Runge et al., "Dark Patterns" in Online Services: A Motivating Study and Agenda for Future Research, 33 Marketing Letters 151–63 (2022).
[27] See Nat'l Acads. of Scis., Eng'g, & Med., Social Media and Adolescent Health (Nat'l Acads. Press 2024)
[28] Cynthia A. Dekker, Susanne E. Baumgartner & Sindy R. Sumter, For You vs. for Everyone: The Effectiveness of Algorithmic Personalization in Driving Social Media Engagement, 101 Telematics & Informatics, art. 102300 (2025).

and track it using the individual's IP address. The platforms may also keep a record of users' frequent purchases and purchasing power. This leads to digital surveillance, which may prove detrimental to individual autonomy.[29]

**The vulnerability of consumers** – The algorithmic personalisation can expose consumers' vulnerability. Data collection by algorithms can reveal users' financial status and other conditions; companies can even infer sensitive aspects of their lives. Such insights can then be used to formulate persuasive methods that may potentially influence consumer behaviour in ways that undermine their autonomy.[30]

**Lack of privacy** – another significant concern is the potential erosion of consumers ' privacy. The extensive collection of data by digital platforms raises concerns about how it will be utilised and the potential for its exploitation. In K.S. Puttaswamy v. Union of India, the Supreme Court held that privacy is a fundamental right of the individual; however, the extensive collection of data by platforms raises questions about the extent to which this right is safeguarded by the digital environment.[31]

It is often argued that consumers are presented with a choice. Their data is collected only after they consent to personalisation. Still, the consumer remains usually unaware of the processes underlying this algorithmic personalisation. The platforms usually treat consumers' agreement as evidence of consent, but consumers are rarely specifically informed about how the platforms will process their data. Such consent cannot necessarily be considered informed when the consumer has no clue, and consent is taken superficially based on only a few facts.[32]

**Towards Meaningful consent: reforms for the digital marketplace**

The existing framework requires reforms to address the emerging challenges arising from digitalisation.

**Moving from click-based consent to meaningful consent**- A critical distinction must be drawn between click-based consent and genuine consent. The mere act of clicking an acceptance button cannot be regarded as conclusive evidence of the voluntariness of a

[29] Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability (May 2014)
[30]Sarita Schoenebeck, Cami Goray, Amulya Vadapalli & Nazanin Andalibi, Sensitive Inferences in Targeted Advertising, 21 Nw. J. Tech. & Intell. Prop. (2024).
[31] K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India)
[32] Digital Personal Data Protection Act, No. 22 of 2023, § 6(1) (India).

consumer's consent to the transaction's implications. The framework shall ensure that the platform discloses the consequences of its conduct, including data collection, payments, processing, and more.

When examining consent, it is necessary to consider the nature of the notices published to obtain it. Certain factors, such as clarity, purpose, accessibility, and the availability of real alternatives, should also be examined. The legal framework should move beyond whether there was acceptance; rather, it should focus on whether the consent was real and voluntary and whether the decision was informed.

**Simplification of digital terms and consent notices**- Platforms frequently rely on lengthy notices filled with complex technical terms. By employing such terminology, the statutory requirement may be met; however, consumers may struggle to comprehend the dense language presented to them, thereby burying important information in jargon.[33]

Therefore, platforms should add clauses explaining the meaning of complex terms and provide a summary in simple language that may include important information about why data is being extracted, how it will be utilised later, its implications after giving consent, and the actual consequences. Also, where platforms offer the option to use the platform in a regional language, they should aim to provide notices in that language to ensure easy understanding for consumers.

**Regulations for the Manipulative Consent interface and dark patterns**- Platforms often design their interfaces in ways that are deceptive and manipulate users' choices. Such practices extend beyond the prominence of the “accept” option over the “reject” options; they also involve misleading visuals and interface designs that manipulate consumers towards specific outcomes desired by the platform. These practices can compromise consumer voluntarism and may affect the eventual outcome.[34]

The existing legal framework includes guidelines under the Prevention and Regulation of Dark Patterns 2023, which recognise and address these challenges.[35] The aim should be to ensure

[33] Omri Ben-Shahar & Carl E. Schneider, More Than You Wanted to Know: The Failure of Mandated Disclosure (Princeton Univ. Press 2014).
[34] Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns, 2023, Annexure I (Nov. 30, 2023)
[35] Id.

that consumers can make choices without design manipulation that is influenced or guided by the platforms.

**Separate consent for separate purposes:** It is often observed that consent to data collection is taken as consent for subsequent use of the data as well. This raises concern, as consent to data collection does not automatically mean consent to subsequent usage of the data.[36]

Therefore, the legal framework must ensure that consent is purpose-specific. Consumers should be provided with separate choices for separate purposes. This method will ensure that platforms stick to the purpose for which consent is obtained and cannot use it as an excuse to escape liability.

**Stronger control over algorithmic personalisation:** As discussed earlier, platforms may monitor a user's search history, location, and purchasing behaviour and then use this data to personalise the feed. Platforms use the collected data to determine content and products tailored to users' preferences, and display a list of options that are already filtered.

Platforms shall be mandated to disclose, in simple language, the personalisation process and provide consumers with the means to disable or modify algorithmic personalisation. Additionally, Consumers should be given sufficient information about the types of data that will be collected.[37]

**Special protection for the digitally vulnerable consumers –** As discussed, a lack of digital literacy makes consumers vulnerable, and, in turn, platforms exploit this fact.

The government should recognise the importance of digital literacy as an essential component of consumer protection in the digital age. Consumers should be equipped to comprehend complex terms and technical knowledge. This can be achieved by integrating this into the school curriculum and public awareness. In this manner, the passive recipients will be converted into active participants, thus reducing information asymmetry and strengthening consumers' ability to make independent choices.

**Stronger remedies and regulatory accountability -** Consumer rights hold little practical

[36] Digital Personal Data Protection Act, No. 22 of 2023, § 6(1) (India).
[37] Fed. Trade Comm'n, A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services (Sept. 2024).

value without an effective enforcement mechanism.

The regulatory framework should incorporate stronger deterrent measures to prevent service providers from violating consumers' rights. The legal framework shall establish clear provisions for mechanisms to withdraw consent, delete data, and cancel subscriptions. Authorities should also examine the platforms' architecture and design interfaces to assess compliance with consumer protection requirements.[38]

**Conclusion**

Digitalisation and the widespread use of technology have transformed the ways consent is obtained. Although consent is relevant and important in contractual agreements, its manifestation through a single click may not necessarily establish expression of a meaningful and voluntary choice.

Standard-form contracts with pre-drafted conditions, manipulative design interfaces on platforms, information asymmetry between consumers and platforms, and algorithmic personalisation methods may undermine the autonomy of consumers, which may raise questions about the efficiency of existing legal protection in addressing the challenges of the digital environment.[39]

Addressing these challenges requires a shift from treating consent as a form of consumer acceptance to actually ensuring that it encompasses a meaningful choice of the individual, which is neither influenced nor affected by other factors.

Ultimately, without meaningful safeguards to ensure meaningful consent, consent risks being reduced to a legal fiction where formal acceptance is made for a voluntary agreement.

[38] Consumer Protection Act, No. 35 of 2019, §§ 18, 20–21 (India); Digital Personal Data Protection Act, No. 22 of 2023, §§ 6(4), 12 (India).
[39] Guidelines for Prevention and Regulation of Dark Patterns, supra note 2.