PRICE OF PLAY: ANALYZING THE LEGAL QUICKSAND OF MICRO-TRANSACTIONS AND IN-APP PURCHASES

Amlan Panda[1], National Law School of India University (NLSIU)

ABSTRACT

The paper deals with the validity of rapid in-app purchases and other micro transactions under the Indian Contract Act. It is argued that the Indian Contract Act is inadequate for addressing the complex and algorithmic nature of the digital transactions. This paper uses both case studies and doctrinal analysis to highlight the deep structural flaws that are present in the Indian framework and the standards used in countries such as EU, Australia and South Korea. In this study, three regulatory gaps emerge: (i) the validity of successive micro-contracts is undermined by the issues of free consent and minor protection, (ii) the lack of any statutory cooling-off period for digital goods leaves the Indian consumers without any withdrawal right, and (iii) the widespread use of 'bundled consent' and 'dark patterns' that manipulate the user's choices and compromises accountability. A feasibility analysis is also conducted to estimate the financial losses emanating out of such flaws. The paper concludes by urging for a modernized legal framework that is on par with the global standards and features bans on bundled consent, mandatory cooling-off periods and tiered consent mechanisms that would result in platform accountability and a safer digital marketplace.

[1] Amlan Panda, National Law School of India University (NLSIU), Bengaluru.

INTRODUCTION:

The advent of the internet era opened the floodgates of a new and enhanced social experience. And this was furthered by the introduction of the online gaming ecosystem which changed the ways of this [newly gained] social experience. And within this ecosystem, there exists a crucial tool that have, off late, become the cornerstone of this experience, i.e., "Microtransactions".

Microtransactions have been perceived as an important source of revenue that has resulted in a rapid transformation of consumers' engagement with the virtual worlds while also providing profitable business models for many gaming studios.[2] These also include "in-app purchases", (which is the focal point of this paper) that are online purchases made by the player (using realworld currency) that provides them with in-app benefits and faster game progression. While this has presented a credible stream for income generation for the corporates, it has also been mired with problems. However, a small [yet crucial] dichotomy has plagued the system – while this has been a win-win situation for both the parties, it has also given birth to a host of new issues that are unconventional and require novel interventions by the legislature. And this is the primary argument that is to be put forth in the next few pages that not only flags the persistence of issues in the current framework, but also suggests some measures for the same.

Firstly, this paper analyzes the current legal framework for the operationalization of digital contracts in the Indian Contract Act (to be herewith referred to as the ICA). *Secondly*, this paper delves into the focal point of the paper i.e. in-app purchases and analyze their validity in the current legal framework. This is done using the ICA as the overarching template to flag out the challenges in the legal validity and enforceability of these micro-contracts and the same is complemented with the use of a real-life case study of games such as Fortnite or Free Fire. *Thirdly*, this paper also explores the concept of "Cooling-off periods" and the challenges faced in applying this to the in-app purchases. Moreover, it also undertakes a comparative analysis of the global approaches in this regard, specifically the European Union (to be henceforth referred to as the EU) regulations and then juxtapose them with the Indian legal jurisdiction.

[2] Ananay Jain, 'Microtransactions in gaming: Striking a balance between profit and player experience' (2024) Grant Thorton <https://www.grantthornton.in/insights/articles/microtransactions-in-gaming-striking-a-balancebetween-profit-and-player-experience/> accessed on 10 February 2025
[This article unveils the underlying debates that have shaped the course of 'microtransactions' in the gaming arena. This article tries to strike a chord with consumer satisfaction, i.e., the experience of the gaming community with the overall monetization trend for the corporates.]

Finally, the paper probes into the concept of "bundled consent" and the lack of any framework for their enforceability and also proposes some guidelines for the same. The paper concludes by summarizing the aforesaid topics and vying for their efficient implementation.

INDIAN CONTRACT ACT (ICA) AND DIGITAL TRANSACTIONS:

The legal framework for enforcing digital transactions in India is guided by the Indian Contract Act (ICA). However, there exists an ambiguity regarding the scope of the application of the Indian Contact Act (ICA) to the current digital transactions, and more specifically microtransactions, since these laws were adopted way back in 1872 when digital transactions were not commonplace. This is problematic since the current system simply relies on the ICA and self-regulatory frameworks which are, most often than not, the discretionary adaptations of the ICA.

This is manifested in the case of *Bhagwandas Goverdhandas Kedia vs. M/S Girdharilal Parshottamdas & Co*[3] (hereafter referred to as the Bhagwandas case) where it was debated as to whether the laws stipulated under the ICA could be extended to digital contracts since the drafters of the statute clearly were unaware of such occurrences.[4] In the aforementioned case, the type of e-contract centered around a telephonic exchange, which is a specie of the genus of "instantaneous communication"[5] and it was opined by the court that the acceptance of any contract that was made using electronic devices such as telex would be construed as complete as soon as it reached the ears of the offeror which, in these cases, would be 'instant'.

This was also furthered by the case of *Entores vs. Miles Far East Corp.*[6] (hereafter referred to as the Entores case) which also reiterated the same judgement that "Postal rule" would not apply to modes of instantaneous communication and since telex [specific to this case] was an instantaneous mode of communication, the postal rule of acceptance would not apply.

---

[3] *Bhagwandas Goverdhandas Kedia vs. M/S Girdharilal Parshottamdas & Co*. [1966] SCR (1) 656

[4] S.Z Amani, 'E-contract in cyber space: Does it really warrant the acceptance of Entores case?' (2007) <https://www.jstor.org/stable/45073187> accessed 11 February 2025

[5] Instantaneous Communication in contract law refers to an offer and acceptance that are made simultaneously, i.e. the contract is formed when the acceptance is received by the offeror. This stands in sharp contrast to the Postal rule that was enumerated in the landmark case of *Adams vs Lindshell* [1818] 1 B & Ald 681 where it was opined that acceptance takes effect when the letter of acceptance has been posted and not when it reaches the offeror. Essentially, this states that acceptance is complete when it is put in the mode of transmission and not when it reaches the other party [offeror]. So, even if it never reaches the offeror or does so after a delay, then it would still be construed that the acceptance has been complete as against the proposer.

[6] *Entores vs. Miles Far East Corp* [1955] 2 QB 327

However, there is yet another aspect that is shrouded in ambiguity. In the context of digital transactions, one crucial aspect is the formation of contracts *sans* geographical limitations. This was contemplated in the Entores case which referred to the case of *Newcomb vs. De Roose*[7] where it was stipulated that the place where the offer has been accepted would be considered as the competent jurisdiction for the contract. This is how the English Common law would determine the jurisdiction of the contract.

However, the Indian perspective was evinced by the [learned] words of Shah, J. in the Bhagwandas case where he opined that Section 4 of ICA[8] did not explicitly specify the need for any jurisdiction for such contracts and only concerns itself with the time of completion of the contract. However, an inimical approach was adopted by Hidayatullah, J. who suggested that Section 4 of the ICA also applies to telephone and wireless communication, while also extending its presence to the realm of e-contracts in the cyberspace.[9]

LEGAL STATUS OF RAPID, SUCCESSIVE MICRO-CONTRACTS:

I. UNDERSTANDING RAPID, SUCCESSIVE MICRO-CONTRACTS:

The concept of microtransactions relate to the purchase [and selling] of virtual goods online, preferably in online games, but can also be applied in the context of IoT (Internet of Things).[10]

Now, to understand the nitty-gritties of micro-contracts, we need to delve into the online gaming experience and how things work over there. And to do this, the paper will use the example of online multiplayer games such as PUBG (Players Unknown Battle Grounds) or Fortnite that provide additional benefits to players when they undertake certain purchases.

---

[7] *Newcomb vs. De Roose* [1859] 2E & E 271
In this case, Hill, J. opined the following:
"*Suppose the two parties stood on different sides of the boundary line of the district; and that the order was then verbally given and accepted. The contract would be made in the district in which the order was accepted.*"
It can be construed to mean that the jurisdiction of the contract would be that of the offeror since the above doctrine stipulates that the contract would be made where it was accepted. However, there exists a dichotomy here since it is unclear whether the doctrine was proposed keeping the "Postal rule" or the "Entores case" in mind.
If the "Postal rule" is considered, then the doctrine stands true. But if we considered instantaneous modes of communication, then it would [purportedly] fall flat since in electronic modes of communication, the jurisdiction is of little to no importance.

[8] Indian Contract Act, 1872 s4

[9] Supra note 4 at 5-7

[10] The terms 'microtransactions' and 'micro-contracts' are not to be confused with. Basically, Microtransactions embody the proceedings that are undertaken following the conclusion of micro-contracts.

The concept of micro-contracts in these online games could be ideated to the smaller, shortterm agreements or tasks that the players can complete to earn rewards or access some additional content over the system. These are smaller in scale as against real-time contracts and are executed with minimal user deliberation. Moreover, they are stealthier and operate in a hidden manner behind the user interface that keeps them out of reach of legal scrutiny. And this is even more problematic when we consider that these are not express contracts, but "quasicontracts" which are embedded within code. This is furthered in the next section that engages with the validity and enforceability of these contracts.

II. CHALLENGES OF THE VALIDITY AND ENFORCEABILITY OF THESE CONTRACTS

It is imperative to question whether these micro-contracts fall under the ambit of quasicontracts before delving into their enforceability. The quasi-contracts are described under Sections 68-72 of the ICA and are obligations imposed by the law to prevent unjust enrichment at others' expense. And the principle of "unjust enrichment" was opined by the Hon'ble Supreme Court in the case of *Mahabir Kishore & Ors. vs. State of Madhya Pradesh*[11] whereby it laid down the necessary elements for the same while upholding restitution.

Hence, the key traits of a quasi-contract could be construed as the following:

(i) *There is no real agreement or consent.*

(ii) *Obligations imposed by the law*

Now, 'micro-contracts' refer to the smaller contracts that are often displayed by most [if not all] of the gaming apps that provide additional content in exchange for real-time currency. It basically provides benefits to the purchasers of these contents and treats them 'special' as against the general players (who don't buy any such packages).

In this case, the Hon'ble Supreme Court ordained the following elements to constitute the principle of "unjust enrichment" and the same are listed down below:

(i) *The defendant has been 'enriched' by receiving a benefit.*

[11] *Mahabir Kishore & Ors. vs. State of Madhya Pradesh* [1989] SCR (3) 596

(ii) *This enrichment has been achieved at the cost of the opposite party, i.e. the plaintiff* (iii) *Retaining the benefit would be construed as 'unjust'.*

(iii) *"Restitutionary" – in the sense that it aims at restoring a benefit that is wrongfully achieved.*

Now, we try and revert back to our gaming example. When a player completes a mission in exchange for in-game currencies or any rewards, then there exists an underlying agreement.

These micro-transactions involve:

- **Offer:** *The game offers a reward for undertaking a mission or task.*
- **Acceptance:** *The player then performs the task which indicates consent.*
- **Consideration:** *Could be either through time, effort or real currencies.*
- **Intention to create legal relations:** *This is arguably absent.*

While these micro-contracts might appear to operate like quasi-contracts, where they lack express negotiation and are often executed automatically, these transactions are, however, backed by implicit consent which makes them closer to informal contracts rather than quasicontracts. Then, we delve into the core legal issue: Whether these micro-contracts are valid and enforceable under the Indian Contract Act?

The question of validity of these micro-contracts is mired with contradictions. While many such contracts meet the [formal] requirements under Section 10 of ICA[12], there still remain infirmities which are revealed on a deeper inspection. Some of these infirmities are discussed below:

FREE CONSENT	This is debatable since consent might be forged due to information asymmetry. Another possible way of hiding consent might be through "Clickwrap agreements"[13] or through at-the-moment purchases in instant gameplay.

[12] Indian Contract Act 1872, s10

[13] Clickwrap agreements are a type of contract in which the user indicates or gives their consent by clicking on a button or checking a box which [often] mentions the following heads: "I Agree", "Accept" etc.

CAPACITY TO CONTRACT	This is also a major issues considering many online multiplayer games are actually played by children under 18 years. Hence, any micro-contracts with such minors are "void ab initio" as per the case of *Mohori Bibee vs. Dharmodas Ghose (henceforth to be referred to as the Mohori Bibee case)*[14].
	Technically, any such purchases made by these minor players create void contracts as per the *Mohori Bibee* judgement. However, the platforms rarely engage in robust age verifications to check and contain such purchases.
BUNDLED CONSENT	Another major issue with microtransactions is the presence of "bundled consent", where the player [typically] agrees to multiple things without clearly understanding even one of them. *This topic is dealt with in detail in the later part of the paper.

Despite the 'prima facie' validity of these micro-contracts, they face enforceability issues under the ICA. From a structural perspective, the enforceability of these micro-contracts is hindered by the legal maxim – *"de minimis non curat lex"* – which translates into – "*the law does not concern itself with trifles".* To substantiate, this maxim acts as a benchmark for the courts to turn down low-value disputes. And this exacerbates the situation because micro-contracts [typically] operate within very little to negligible monetary units and hence this doctrine [effectively] acts as a shield for all such gaming platforms.

Furthermore, there are inadequacies within the ICA that fails to account for the dynamics of micro-contracts. While the statute addresses core legal issues, it [still] does not account for automated & algorithmic offers and consent that is obtained through deceptive UX/UI designs. The Consumer Protection Act, 2019[15] does provide some coverage to such digital agreements

[14] *Mohori Bibee vs. Dharmodas Ghose* AIR 1903 PC 88
[15] Consumer Protection Act 2019

and also includes suitable mechanisms under the E-Commerce Rules, 2020[16]. Yet, it fails to address repetitive micro-contracts and the regulation of such microtransactions.

The Information Technology Act, 2000[17] also deals with data security under Section 43A[18] but does not regulate digital contracts and treats platforms as neutral parties instead of contractual intermediaries, thereby allowing them to evade accountability.

III. THE RISK OF CONSUMER EXPLOITATION AND STRUCTURAL GAPS:

This section furthers the lack of judicial intervention in the domain of microtransactions and also delves into the paucity of any relevant doctrine that is tailored for such digital environments.

Microtransactions are not traditional contracts, rather are emanated out of manipulative digital environments. This is exemplified by the use of UI (User Interface) elements that trick users into unintended purchases. And these purchases are sustained using artificial urgencies such as time-limited events. Moreover, by obscuring the distinction between actual currencies and ingame currencies, the platforms are inducing this involuntary spending.

Furthermore, this irrational behaviour, which is sustained using unfair algorithmic practices, is [indirectly] fostered due to a lack of support from the Indian legal system that provides an incentive for the platforms to evade liability. This structural opacity has raised normative concerns. For example, while the games are advertised as 'free', they exploit the data amassed by their platforms, such as engagement habits, to offer player-specific game simulation such as special offers and effects. These behavioral patterns are then used by such gaming platforms to refine their strategies for effective monetization. And this entire process lacks "granular consent" that creates a hidden cycle of consumer exploitation.

'Granular consent' is a model that is based on informed user consent, wherein the users are [independently] allowed to agree or disagree based on different components or services. This is specifically important because granular consent breaks down user consent into distinct categories such as consent to data collection, consent for sharing this data with third parties, etc. And this allows the users to accept all these terms individually and to choose which

[16] Consumer Protection (E-Commerce) Rules 2020
[17] The Information Technology Act 2000
[18] The Information Technology Act 2000, s43A

permissions they are comfortable with. This stands in contrast with the common practice of forcing the users to accept all these terms in a single click.

This is also a recognized principle under the Digital Personal Data Protection Act, 2023 (hereafter to be referred to as the DPDP Act)[19] because most of the platforms are using bundled consent which means that users cannot play without agreeing to such practices. And this principle has got statutory backing from Section 6(1) of the DPDP Act[20]. Thus, mandating granular consent would ensure more valid microtransactions and also reduce the risk of consumer exploitation.

IV. CASE STUDY [PUBG] (Players Unknown Battle Grounds)

PUBG (Players Unknown Battle Grounds) is a multiplayer game that operates on a 'freemium' model where players can play for free but are [constantly] encouraged to make in-app purchases for cosmetic upgrades in the game. And most of these upgrades are paid for using in-game currencies, which are in turn purchased using real currencies.

A typical in-app purchase in PUBG involves buying loot boxes using in-game currencies (bought by real currencies) where no-refund is available and the player has no [clear] information about the odds of receiving the desired item.

The purchase system in PUBG echoes the model of 'bundled consent' where the user involuntarily [and unknowingly] consents to a range of actions such as behavioral data collection, data sharing with third parties, waiver of statutory rights such as the right to refund or dispute resolution etc. And this stands in sharp contrast with the DPDP Act[20] that prohibits non-specific consent. Moreover, a large user base of PUBG comes from the age group of under 18 years; yet it permits purchases without age verification and parental oversight. Thus, any such consent is void as per Section 11 of the ICA[21]. However, it escapes legal scrutiny because these transactions are so small that enforcement becomes [almost] impractical.

[19] Digital Personal Data Protection Act 2023
[20] ibid s6(1)
[20] Digital Personal Data Protection Act 2023
[21] Indian Contract Act 1872, s11

For example, if a user were to ask for a refund for a Rs. 80 loot box, the courts may refuse to hear the matter since the law does not involve itself in trifles. Thus, the transaction remains insulated from consumer protection, despite illegality of the same from a technical perspective.

Therefore, this model points to larger structural opacity in digital marketplaces and it aptly manifests how legal doctrines are regularly being outpaced by platforms, which is creating a perfect quicksand for the consumers.

APPLYING COOLING-OFF PERIODS TO MICRO-TRANSACTIONS

I. CONCEPT OF COOLING-OFF PERIODS:

The concept of "cooling off period" refers to a [clearly defined] window during which the consumer can cancel a purchase without being penalized. This is crucial for protecting the consumers from manipulative tactics and also giving them a window to reconsider their purchase.

After making a microtransaction, the user [in this case] has a set window within which the user can either request for a refund or cancel the transaction altogether. This process ensures that the consumer is not exploited by digital platforms by using UI manipulation such as timelimited offers. Moreover, major platforms such as Google, Apple, Steam etc. have also set their own cooling-off periods.

To illustrate this, if a user buys some items [such as in-game skins] in a mobile game, then the 'cooling-off period' helps the user to ask for a refund if they do not use the item. Once the period expires, the consumer loses the right to cancel the transaction. Thus, 'cooling-off periods' aim to balance the consumer protection with fair business practices within the digital environment.

II. CHALLENGES OF IMPLEMENTING COOLING-OFF PERIODS TO MICROTRANSACTIONS:

However, implementing 'cooling-off periods' for microtransactions faces numerous hurdles in technical and legal dimensions. Some of these challenges are enlisted below:

(i) In-game purchases deliver the items immediately, hence making it difficult to

enforce as they might have been consumed. And once these items have been used, it becomes difficult to redeem same, thereby complicating the refund process. This puts the onus on the platforms to decide whether the goods should be immediately put to use or should be 'frozen' during the cooling-off period.

(ii) The implementation of this concept requires [technical] adjustments to the platforms in order to handle their transactions while also managing refunds in a parallel manner. And this requires significant investments to build and operate which is possible only for big corporates and smaller platforms [or startups] stand at a disadvantage.

(iii) Another hindrance of implementing 'cooling-off periods' is that users might purchase digital goods, use them and then ask for a refund, all while the cooling-off period persists. This creates a hassle for platforms to track and prevent funds to such users while legitimate ones suffer due to this process.

(iv) A large part of these micro-contracts [or in-app purchases] are undertaken by younger audiences who are not well versed with the implications of these 'coolingoff periods.' Moreover, many of these purchases are made without explicit parental consent which further exacerbates their vulnerability.

(v) Furthermore, rapidly evolving business models such as non-fungible tokens (NFTs) which operate on blockchain technologies further pose a serious challenge to the implementation of cooling-off periods. Blockchain makes it virtually impossible to identify and track the chain of transactions or the purchasers which jeopardizes refund and creates uncertainty for developers and users alike.

III. POTENTIAL WAYS OF IMPLEMENTATION:

In spite of the aforementioned challenges, the implementation of 'cooling-off periods' requires a blend of policy initiatives and statutory interventions. Some of these ways are discussed below:

(i) One of the most obvious ways could be determining a specific time frame within which the users can ask for a refund. This can be aligned with the practices in the

European Union (EU) Consumer Rights Directive (2011/83/EU)[22] where there is a 14-day withdrawal period for the consumers. This provides for user protection within a stipulated period, thereby balancing both consumer and business interests.

(ii) Another way could be informing the parents within a 24-hour timeline about the purchase made by their children with the option of cancelling it through email or some other way as is stipulated in the communication. This allows parents to regulate spending by minors. However, this would require robust age verification and parental-linkage systems to approach the 'legal' guardians. Moreover, if the purchased item has been used by the minor, then that raises serious questions about refund processes.

(iii) Referring to the aforementioned problem, one possible method could be adjusting the refund processes to act on a pro-rata basis i.e., the users receive a proportional share of the refund of the unused part of the item or service.

(iv) The platforms could also 'freeze' the items for a short-time, immediately after the transaction, to ensure that the consumer is not indulging in impulsive transactions and it also acts as a potential barrier for preventing use-and-return of items by consumers.

IV. GLOBAL APPROACHES AND COMPARATIVE ANALYSIS WITH THE INDIAN JURISDICTION:

(i) European Union (Directive 2011/83/EU – Consumer Rights Directive):

The European Union (EU) provides cooling-off periods to consumers in digital transactions unless the user [explicitly] agrees to waive it. The EU Consumer Rights Directive (2011/83/EU)[23] provides for a 14-day withdrawal period for distance contracts (which also includes microtransactions within its ambit).[24]

[22] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC and repealing Council Directive 85/577/EEC and Directive 97/7/EC [2011] OJ L304/64 https://eur-lex.europa.eu/eli/dir/2011/83/oj/eng

[23] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC and repealing Council Directive 85/577/EEC and Directive 97/7/EC [2011] OJ L304/64 https://eur-lex.europa.eu/eli/dir/2011/83/oj/eng ¶ 40

[24] ibid https://www.legislation.gov.uk/eudr/2011/83/body ¶ Article 9 [Right of withdrawal]

However, the right does not apply to transactions where the consumer gives prior consent to lose his/her withdrawal right as per Article 16(m) of the Directive.[25] And this is further supported by Article 6(1)(h) of the Directive and Annex I.[26] Thus, the emphasis in this case is on making informed consent by placing procedural safeguards to protect the consumers rather than prioritizing speed.

In the Indian jurisdiction however, there is no express cooling-off period either in the Consumer Protection Act, 2019 (CPA), or Digital Personal Data Protection (DPDP) Act, 2023. The consent standard in India is typically bundled with an absence of withdrawal rights. While the EU follows granular consent and procedural fairness, India prioritizes platform discretion where refund rules are vague and lightly-enforced.

(ii) Australia (Competition and Consumer Act, 2010; Schedule 2 of the Australian Consumer Law):

In this case, the refund framework does not expressly specify cooling-off periods for digital transactions. Instead, it laid down consumer standards and the services must fulfill certain descriptions to be of an acceptable quality to be consumed by them. Section 54 of the Competition and Consumer Act, 2010[27] stipulates the qualitative requirements and Section 55 of the Act[28] provides for a guarantee for the fitness of purpose for the purchase. Moreover, Section 259 of the [said] Act[29] also allows for refunds if the guarantees, pertaining to both the quality and purpose of the items, are breached.

Australia offers remedies based on consumer expectations and if the products or services do not fit the qualitative dimensions, then refunds could be demanded. On the contrary, clear proof of defect is required to ask for remedies in India, which is often difficult to establish in microtransactions. In Australia, the enforcement is regulated by the Australian

---

This article stipulates that the user shall have 14-days as the withdrawal period for a distance contract and the member states of the European Union (EU) shall not prohibit the parties from performing their obligations.

[25] ibid ¶ Article 16(m)
This clause expressly mandates that if the content is delivered online i.e., it is not delivered in a physical medium, then the consumer loses the right to cancel the delivery of the item if they gave clear permission to waive their right of withdrawal.

[26] ibid ¶ Article 6(1)(h) and Annex I(B)
It stipulates that the trader shall expressly point out whether a right of withdrawal exists and the procedures for exercising the same in tandem with Article 11(1) of the Directive. The withdrawal form is presented in Annexure I(B).

[27] Competition and Consumer Act 2010, s54

[28] Competition and Consumer Act 2010, s55

[29] ibid s259

Competition and Consumer Commission (ACCC) but no such enforcement authority exists in India and the Consumer Commissions are overburdened and not fit to regulate tech abuse. Moreover, the Australian approach is reactive i.e. the rights activate when the products fail to match consumer expectations. However, the Indian approach is limited and requires the consumers to prove the breach.

(iii) South Korea (Act on the Consumer Protection in Electronic Commerce, etc., Game Industry Promotion Act):

South Korea has adopted sector-specific laws such as the Act on the Consumer Protection in Electronic Commerce (to be hereafter referred to as the E-commerce Act)[30] and the Game Industry Promotion Act (to be referred to as GIPA)[32] to regulate digital content. Article 17(1) and (3) of the E-Commerce Act[31] provides for a 7-day withdrawal period unless the product has been consumed. Moreover, Article 24(2) of GIPA requires the platforms to include refund policies in [unused] in-game items. One of the crucial distinctions in the South Korean model is platform accountability, i.e. obligations to provide refunds is imposed on the platforms. This is evident in their regulatory approach where they follow an *"ex ante model*" which provides for pre-purchase disclosures and 'cooling-off periods' [Article 17 of the E-Commerce Act] to prevent harm.

In contrast, digital transactions are treated in the same manner as physical goods in the Indian jurisdiction, thereby creating a grey area in regulating such microtransactions. Moreover, there are no statutory rights that provide for withdrawal periods in digital goods. A pertinent thing to note is that the Consumer Protection Act, 2019 (CPA) does provide for refunds for either "defective goods" [Section 2(10)[32]] and "deficient goods" [Section 2(11)[33]]. This is problematic since it does not clearly distinguish between used and unused goods. And this makes the Indian regulatory approach vague due to no clarity in statutory rules.

Furthermore, in India, the platforms are [largely] viewed as 'intermediaries' and hence no

[30] Act on the Consumer Protection in Electronic Commerce 2012
[This Act commenced on 30th March, 2002 and was fully amended by Act no. 11461 on 1st June, 2012]
[32] Game Industry Promotion Act 2018
[31] Act on the Consumer Protection in Electronic Commerce 2012, Article 17(1) and (3)
[32] Consumer Protection Act 2019, s2(10)
[33] Consumer Protection Act 2019, s2(11)

direct liability is imposed on them. This facilitates their escape by shielding their obligation to offer refund systems. And the enforcement framework in India is ill-suited to address digital discrepancies either due to lack of enforcement mechanisms or overburdened consumer redressal forums. Thus, India continues to prefer contractual clarity over user protection.

DELVING INTO BUNDLED CONSENT IN MICROTRANSACTIONS:

I. CONCEPT OF BUNDLED CONSENT:

The concept of 'bundled consent' refers to a locus of giving consent where the user [involuntarily] provides an all-encompassing consent to a range of services without the ability of choosing specific terms or services. This type of consent is non-granular, i.e., users must agree to all the terms in order to proceed. Bundled consent is problematic because it enables:

(a) Purchases which were not intended to be purchased in the first place.

(b) A broader ambit of the consent given

(c) Implicit and involuntary authorizations for automatic updates without engaging the user.

(d) UI/UX design manipulation that hides transactions and subvert user autonomy.

Moreover, the CCPA's Guidelines for the Prevention and Regulation of Dark Patterns[34] also [implicitly] classifies bundled consent as a specific dark pattern under Annexure I of the guidelines. A crucial thing to note is that the CCPA had issued these guidelines in the context of data protection but these could be extended to include in-app purchases and other microtransactions, as is specified under Section 3 of the guidelines.[35]

'Bundled consent', technically, does not fall under any distinct category of dark pattern in Annexure I of the guidelines. Instead, it could be construed as a mixture of a set of categories. To substantiate, clauses (iv) and (vi) of the guidelines which talk about 'forced action' and

[34] Guidelines for Prevention and Regulation of Dark Patterns 2023
[35] ibid s3

'interface interference' could be interpreted to mean bundled consent. The logic of the guidelines could be extended because the users are not provided separate options and broader consent agreements are grouped by utilizing the same consent, thereby obscuring consumer choice.

II. LACK OF FRAMEWORK AND LEGAL GREY AREAS:

The problem in regulating bundled consent is the lack of definitions of the same in the Indian laws. And this causes the users to [unknowingly] agree to terms such as automatic subscription renewals and third-party data sharing. Moreover, the E-Commerce Rules, 2020 applies only to marketplace and not app ecosystems. And with no regulatory authority to oversee platform ethics, the microtransactions are not invalidated unless the fraud is expressly proved. Even under the DPDP Act, 2023[36], the consent framework is data-centric and not transaction-centric which means that the payments are not regulated as such.

Furthermore, the Indian regulators have not issued any binding rules and guidelines on manipulative UI/UX practices which lead to unintentional purchases. Although the CCPA guidelines[37] do [implicitly] recognize bundled consent as a "dark pattern", but they operate in an advisory role and are not legally binding or enforceable. Hence, there exists a legal grey zone due to a clear lack of any [relevant] doctrinal standard for the same.

India [currently] lacks a proper legal framework that:

(i) Requires pre-purchase disclosures

(ii) Defines or prohibits "dark patterns" and

(iii) Advocate for granular opt-ins instead of bundled consent.

Moreover, there is a lack of clarity on the imposition of liability when a user is misled to make a purchase or when a refund is not arranged for despite the lack of proper disclosure. And this results in 'procedural dead ends' that discourages consumers from seeking redressal against unethical practices. Thus, the consumers are caught in a 'grey zone' where they are deemed to

[36] Digital Personal Data Protection Act 2023
[37] Guidelines for Prevention and Regulation of Dark Patterns 2023

have given the requisite consent, but that was not informed and shrouded in ambiguity and there is no immediate remedy for the same under the Indian laws.

III. LEGAL AND ETHICAL IMPLICATIONS:

The purported 'grey zone' has both legal and ethical issues arising from it, mainly due to the violation of free and informed consent [as stipulated under the Indian Contract Act, 1882 (ICA)]. And bundled consent violates both the parameters of providing sufficient information and specificity of the information concerned since they are usually buried deep within the broader terms of service. This, in turn, compromises the user's ability to comprehend what they are agreeing to, thereby aiding platforms to sidestep granular opt-ins and go for an architecture that leverages interface manipulation to induce fast interactions.

This problem is particularly acute when vulnerable users such as children [who form the majority of the user base of these games and streaming platforms] are considered. A typical form of sidestepping utilized by the platforms include faulty age verification frameworks where no real-time verification such as biometric authentication (Aadhar in the case of India) is used. This is further compounded by the 'bundled payment gateways' which use "dark patterns" such as artificial scarcity to induce impulsive purchases. And the absence of any statutory coolingoff period or clear regulations on consent standards mean that the users are [often] left without remedies. Therefore, these gaps point out to a systemic failure plaguing India's emerging platform economy.

IV. PROPOSING AN ALTERNATE FRAMEWORK:

In India, with a burgeoning digital gaming and platform industry, there is an immediate need of a tailored user protection framework. Hence, I propose an alternate framework that combine procedural simplicity and financial viability that will help in regulating consumer behaviour and redressal against potential harms.

To start with, 'bundled consent' must be considered as a distinct regulatory hurdle that can be notified within the Consumer Protection Act or Digital Personal Data Protection Act to ensure statutory backing and proper redressal mechanism. The wordings of the definition must also be broad enough to cover all the possible activities within its ambit. Moreover, a mandatory cooling-off period for all digital platforms [preferably a 24-hour window] should be introduced

where the users can cancel and request for a refund within the stipulated time frame. This refund framework could be made more effective by integrating automated workflows that make this system responsive and cost-effective at the same time.

Furthermore, a tiered mechanism for microtransactions could be adopted for user protection and smooth platform experience, instead of the adoption of granular consent which makes it cumbersome while also disrupting the services. This could be adopted in the following manner:

TIER	**TYPE OF CONSENT REQUIRED**
Tier 1	*This is where the **initial disclosure** takes place and explicit consent of the user is asked before proceeding on to the services. For example, the notification to accept or reject all cookies where the user is asked to give clear and unambiguous consent.*
Tier 2	*This tier can be ideated to "**session-based consent**". This is granted for a limited time period, thereby allowing for better user experience. For example, the site might ask "Do you want us to remember your settings for this visit only?"*
Tier 3	*This tier is put in place to handle **recurring small purchases** that take place on the website. This allows the users to undertake low-value purchases within a pre-*
	set ambit. For example, the platform might display the following notification: *"Allow essential cookies only/ remember the settings for future use."*

Moreover, the platform accountability model that currently holds [only] the developer accountable must be expanded to also include app-hosting platforms such as Google Play or Apple App Store to ensure shared responsibility and more robust gatekeeping mechanisms. The hosting platforms should verify whether or not the app integrates the aforementioned tiered mechanism and a proper refund system before hosting it. And any failure to do the same would

result in penalties and even delisting the apps from the platform.

As for the enforcement mechanisms, the government should set up an online portal, preferably under the Department of Consumer Affairs, where the users can file complaints. And the system must be designed with an automated grievance aggregation model that identifies and groups the cases based on their amount, the type of action demanded etc. which would lead to systemic enforcement. And this would relieve the pressure from the courts or commissions, who can then focus on the more pressing issues.

FEASIBILITY ANALYSIS:

I. STATISTICAL FEASIBILITY:

India is one of the fastest growing digital ecosystems with a burgeoning gaming and app industry with an estimated user base of around 590 million gamers in FY 2024.[38] Moreover, the skyrocketing of UPI transactions[39] manifests a growing transactional environment that includes [but is not limited to] online content subscriptions, microservices, gaming subscriptions etc. And this highlights the need for appropriate safeguards for user safety.

For example, the gaming industry in India, which has one of the largest user bases in the world, had generated a revenue worth $3.8 billion in FY2024 (~ 23% YoY growth).[40] This growth was possible due to the surge in in-app purchases, which registered a 41% YoY growth. Moreover, this segment is expected to grow with a compound annual growth rate (CAGR) of 34% in the next 5 years.

If we delve deeper into these transactions, it is observed that the Average Revenue Per Paying User (ARPPU) has also witnessed a sound jump, with a 15% YoY increase to $22 in FY2024.[41] And the emergence of digital payment options such as the UPI has only helped the process.

[38] Aryaman Gupta, 'India's Online gaming market grew by 23% in FY24 despite GST burden' *Business Standard* (New Delhi, 11 November 2024) < https://www.business-standard.com/industry/news/gaming-marketto-grow-at-25-to-9-2-bn-by-fy29-despite-gst-burden-report-124111100496_1.html>
[39] Allirajan Muthuswamy. 'UPI: The world's favourite payment method hits $964 billion in record time' *Livemint* (30 August 2024)
[40] Aryaman Gupta, 'India's Online gaming market grew by 23% in FY24 despite GST burden' *Business Standard* (New Delhi, 11 November 2024)
[41] Vikas SN, 'India's gaming market to reach $9.2 billion by FY29, in-app purchases to drive growth' *Moneycontrol* (11 November 2024)

II. FINANCIAL ANALYSIS:

India is witnessing a rapid digital transformation where there is a sound online user base. Hence, even a small error might lead to huge financial repercussions and can affect millions. To understand this in depth, let us assume that around 2% of the 590 million users face some unethical practices or [accidental] transactions due to manipulated consent.

This translates to around 12 million (11.8 million users to be exact) users being affected. Now, we further assume that each of these [affected] users face an average of unwanted microtransactions amounting to $1 (~86 INR). Therefore, the total financial impact equates to:

- Total financial impact = $1 * 11.8 million = $11.8 million/year

  = 86 INR * 11.8 million = Rs. 101.48 crores/year

And this is a highly conservative estimate. The numbers are huge, even if 10% of these users face such irregularities. These figures highlight the extent of digital manipulation and the [urgent] need for user protection measures. As is visualized above, even a small percentage of these unethical practices can cause major harm to India's vast and growing digital populace. Therefore, it is pertinent for the policymakers and regulators to ensure transparent consent mechanisms and stronger accountability frameworks to ensure that India's digital growth story remains both inclusive and trustworthy!!

CONCLUSION:

Therefore, this paper exposes the growing gap between the outdated Indian legal frameworks and the realities of the digital marketplace. As was discussed at length, the Indian Contract Act, 1872 fails to address the microtransactions that are driven by manipulative design, bundled consent, etc., that are issues that undermine both free consent and consumer protection. Thus, the users are left vulnerable since the statutes are devoid of any right to withdraw from sham digital purchases when compared to international standards such as in South Korea or the European Union.

This study reveals that the unethical transactions on the digital medium could affect millions, and the same also calls for the urgent need for reform. Hence, this paper proposes a new regulatory model that emphasizes greater platform accountability, tiered consent mechanisms

and cooling-off periods, thereby aligning the Indian legal frameworks with the global standards. And addressing these issues can turn India's "*legal quicksand*" into a firm foundation for a transparent and equitable digital economy.

BIBLIOGRAPHY:

1. Indian Contract Act, 1872
2. Consumer Protection Act 2019
3. Consumer Protection (E-Commerce) Rules 2020
4. The Information Technology Act 2000
5. Digital Personal Data Protection Act 2023
6. Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC and repealing Council Directive 85/577/EEC and Directive 97/7/EC

   [2011] OJ L304/64 https://eur-lex.europa.eu/eli/dir/2011/83/oj/eng
7. Competition and Consumer Act 2010
8. Act on the Consumer Protection in Electronic Commerce 2012
9. Guidelines for Prevention and Regulation of Dark Patterns 2023
10. Game Industry Promotion Act 2018
11. *Bhagwandas Goverdhandas Kedia vs. M/S Girdharilal Parshottamdas & Co*. [1966] SCR (1) 656
12. *Entores vs. Miles Far East Corp* [1955] 2 QB 327
13. *Newcomb vs. De Roose* [1859] 2E & E 271
14. *Mahabir Kishore & Ors. vs. State of Madhya Pradesh* [1989] SCR (3) 596
15. *Mohori Bibee vs. Dharmodas Ghose* AIR 1903 PC 88
16. Ananay Jain, 'Microtransactions in gaming: Striking a balance between profit and

player experience' (2024) Grant Thorton

<https://www.grantthornton.in/insights/articles/microtransactions-in-gaming-strikinga-balance-between-profit-and-player-experience/> accessed on 10 February 2025

17. S.Z Amani, 'E-contract in cyber space: Does it really warrant the acceptance of Entores case?' (2007) <https://www.jstor.org/stable/45073187> accessed 11 February 2025

18. Aryaman Gupta, 'India's Online gaming market grew by 23% in FY24 despite GST burden' *Business Standard* (New Delhi, 11 November 2024) < https://www.businessstandard.com/industry/news/gaming-market-to-grow-at-25-to-9-2-bn-by-fy29despite-gst-burden-report-124111100496_1.html>

19. Allirajan Muthuswamy. 'UPI: The world's favourite payment method hits $964 billion in record time' *Livemint* (30 August 2024)

20. Vikas SN, 'India's gaming market to reach $9.2 billion by FY29, in-app purchases to drive growth' *Moneycontrol* (11 November 2024)