TERMS & CONDITIONS ARE MAKING A MOCKERY OF CONSENT: A LEGAL ANALYSIS

Swetha M, LLM, JAIN (Deemed-to-be University), School of Law, Shankarapura, Bengaluru, Karnataka 560004

Joy Naresh P N, LLM, JAIN (Deemed-to-be University), School of Law, Shankarapura, Bengaluru, Karnataka 560004

ABSTRACT

Online contracting has produced a quiet but serious crisis in how we think about consent. The people most exposed to digital agreements are, almost without exception, those least positioned to actually read or understand them. This article looks at how dark patterns deliberate choices in interface design and contract drafting hollow out the consent requirement that lies at the heart of contract law. Drawing on doctrine, user behaviour research, and regulatory developments in the US, EU, and India, it maps the specific mechanisms at work: documents engineered to resist reading, high-stakes clauses buried where no one will find them, interfaces that make clicking agree effortless while making withdrawal needlessly difficult, and terms that update themselves through the legal fiction of inaction. Courts have not been equal to this challenge. The clickwrap/browse wrap line drawn in cases like Specht v. Netscape and Nguyen v. Barnes & Noble provides some guidance, but unconscionability doctrine the most natural common law vehicle for relief has been substantially neutered, particularly since AT&T Mobility v. Concepcion. The GDPR, California's privacy statutes, and India's DPDPA 2023 represent real progress, though enforcement remains patchy. This article closes with a four-part reform agenda: mandatory plain language, machine-readable disclosure standards, judicial recalibration, and a serious reckoning with what professional responsibility actually requires of lawyers who draft these instruments.

Keywords: Dark Patterns, Informed Consent, Digital Contracts, Clickwrap, GDPR, DPDPA 2023, Unconscionability, Consumer Protection, Platform Regulation, Data Privacy.

I. Introduction

On billions of devices, every single day, the same thing happens. A user reaches the end of a sign-up flow, sees a block of dense text they were never going to read, and clicks Accept. Nobody stops them. The law, in fact, encourages it treating that gesture as a binding commitment capable of waiving litigation rights, authorising commercial exploitation of personal data, and enrolling the person into obligations they have never encountered and, in many cases, could not interpret even if they tried. The gap between what courts say that click means and what the person doing the clicking actually experiences is one of the stranger unresolved problems in private law today.

The numbers are revealing. A Carnegie Mellon study calculated that an average American internet user who tried to read every privacy policy they encounter in a year would spend around 76 full working days doing so. [1] and that's only privacy policies. It leaves out terms of service, end-user licence agreements, cookie banners, and the rest of the legal architecture platforms use to assert authority over their users. Put together, the body of legal text an ordinary person is deemed to have accepted through routine internet use is simply not readable not in any time frame a real person has available.

When platforms point to user consent to justify monetising personal data, blocking class actions, or rewriting their own terms mid-relationship, they are invoking something that almost never actually occurred. The consent is a legal label attached to a moment of inattention. Courts and lawyers know this. The technology companies who benefit from the current arrangement certainly know it. Yet the law has been slow to say so openly, and the commercial incentives for maintaining the fiction run in one direction only.

This article takes the position that this has to change, and that doctrine, regulation, and legal practice each have a role to play. Part II explains what dark patterns are and why interface design has always been a legal question, even when courts have treated it as someone else's problem. Part III catalogues the main mechanisms through which meaningful consent gets replaced by formal assent. Part IV looks at how existing doctrine handles and largely fails to handle the resulting agreements. Part V surveys the regulatory landscape in three jurisdictions. Part VI examines how the major platforms have behaved in practice. Part VII raises some professional ethics questions that pure compliance analysis tends to skip. Part VIII proposes a reform framework. Part IX concludes.

II. What Are Dark Patterns — And Why Should Lawyers Care?

Harry Brignull coined the term 'dark patterns' in 2010, after spending years cataloguing interface designs that shared a common purpose: they were built to serve the platform, not the person using it.[2] His taxonomy covered the predictable categories sign-up flows that are easy, cancellation flows that are not; layouts that guide attention toward the preferred option while making the alternative hard to find; checkout screens that hide the real price until the user is too invested to walk away. The framework stuck because it gave practitioners a precise vocabulary for something they had been observing without quite being able to name.

Legal academics were slower to the topic. For a long time, the working assumption in contract doctrine was that interface design was a product matter, not a legal one that enforceability turned on what the text said, not on how the page was laid out. Hartzog challenged this directly. His argument was simple: every visual and structural choice in an interface encodes a preference about whose interests get served. [3] That encoding has legal consequences when it shapes the conditions under which someone agrees to be bound. Ignoring design choices is not doctrinal neutrality; it is a choice to ignore evidence.

The problem sharpens considerably when dark patterns appear inside the contract itself rather than just in the surrounding interface. A terms document designed to be too long and too dense to read is not merely inconvenient design. A mandatory arbitration clause positioned to avoid detection is not just bad typography. A consent toggle that defaults to sharing and resists change is not an aesthetic choice. Each of these is a deliberate structural decision to prevent the other party from knowing what they are agreeing to which is precisely the opposite of what a valid agreement requires. [4]

III. Manufactured Consent: The Principal Techniques

A. The Wall of Text

Start with sheer length. Apple's iTunes terms once ran past 20,000 words.[5] PayPal's user agreement has exceeded 36,000. [6] A study tracking the actual online behaviour of over 48,000 US households found that users accessed licence agreements before software downloads in well under one per cent of observed transactions. [7] These figures are not surprising. Reading a 36,000-word legal document before downloading an app is not a realistic expectation and the

companies writing these documents know it. The length is not accidental. Long documents serve a purpose: they create space to bury terms that users would refuse if they saw them plainly stated, while still satisfying the formal requirement that terms were made available.

This is not conjecture. The same legal teams that produce impenetrable consumer-facing agreements write clear, readable documentation for investors and regulators. The language barrier is a choice, not a constraint.

B. Legalese as a Structural Barrier

Even setting aside length, the language itself excludes. Platform contracts typically use passive constructions that hide who is doing what, heavily cross-referenced definitions that require moving back and forth through the document to decode any single sentence, and technical formulations that have no equivalent in ordinary speech. Marotta-Wurgler's research found that even deliberate simplification efforts produced only modest gains in user comprehension.[8] This matters. If genuine readability improvements don't move the needle much, the underlying problem isn't just that words are hard it's that the whole system, from document length to presentation context to time pressure, is oriented against understanding. Opacity is not a side effect of legal drafting. It's a feature.

C. Strategic Burial of Consequential Clauses

Where a clause sits in a document is not an arbitrary decision. Platforms consistently place their highest-stakes provisions mandatory arbitration, class action waivers, broad data-sharing authorisations, unilateral modification rights, auto-renewal terms in sections that come late in documents already too long to read. The terms are technically present and formally agreed to. But their placement reflects a clear-eyed bet that virtually no user will ever reach them. Formal availability and practical invisibility are not the same thing, even if contract doctrine has often been willing to treat them as though they are.

D. The Illusion of Choice: Take It or Leave It

Adhesion contracts are not new, and neither is the concern that one-sided standard-form agreements deserve closer scrutiny. But the coercive quality of digital adhesion is of a different order. If the service at stake is an operating system that came pre-installed on a device you paid for, or an email platform your employer mandates, or the social network where most of your

professional and personal relationships now live, the theoretical option to decline is hollow. Exit isn't free. It costs relationships, professional functionality, access to markets. No market-choice model built on the assumption that consumers can simply switch adequately accounts for those costs.

E. Consent by Inaction and Unilateral Modification

Perhaps the most legally audacious mechanism is also the most normalised: the practice of sending users a bulk email or in-app alert notifying them of revised terms, then treating their continued use of the service as acceptance. No box to check. No confirmation required. A user who missed the notification entirely or saw it and didn't understand what non-action would mean is nonetheless held to have consented to whatever changes the platform decided to introduce. Once consent can be inferred from silence, the idea of an agreed-upon set of terms becomes largely fictional.

IV. The Legal Question: Is Any of This Actually Valid?

A. The Clickwrap and Browse wrap Distinction

US courts have drawn a basic line between clickwrap and browse wrap. Clickwrap requires some affirmative step a box checked, a button clicked before proceeding. Browse wrap simply declares that using the site constitutes acceptance, whether or not the user ever saw the terms. The distinction matters in principle, but the case law applying it is less coherent than it might appear.

In Specht v. Netscape, the Second Circuit refused to enforce an arbitration clause buried in a licence agreement reachable only by scrolling past the download button to a hyperlink most users would never find. [9] the court said this wasn't conspicuous enough. In Nguyen v. Barnes & Noble, the Ninth Circuit said much the same thing about terms-of-service links sitting unannounced at the bottom of a webpage. [10] Then in Meyer v. Uber, the same court went the other way enforcing an arbitration clause because small but readable text near the registration button mentioned that terms applied. [11] The line between these outcomes is not a principled one. It comes down to pixel-level visual assessments that courts are not well-equipped to make, and it provides neither side with much certainty.

The deeper problem is the market-exit logic courts have borrowed from Judge Easterbrook's

ProCD v. Zeidenberg opinion: the idea that someone who dislikes the terms can simply return the product. [12] That reasoning made limited sense in 1996 for shrink-wrap software. It doesn't travel well to a world in which the service you're supposedly free to leave is your professional email, your smartphone operating system, or the network connecting you to your entire social and professional life. When leaving isn't a real option, the theoretical freedom to leave is not a safeguard.

B. Unconscionability and Its Limits

Unconscionability looks, on paper, like a promising avenue. Leff's framework asks two questions: were the formation conditions unfair (the procedural dimension), and are the terms themselves oppressively one-sided (the substantive dimension)?[13] Digital consumer contracts score badly on both counts extreme informational asymmetry, no negotiating capacity on the consumer side, studied linguistic complexity, provisions that eliminate core legal rights. Yet the doctrine has not delivered much relief, and the principal reason is AT&T Mobility v. Concepcion. The Supreme Court's holding that the Federal Arbitration Act pre-empts state unconscionability doctrine as applied to class arbitration waivers has effectively put the most common type of objectionable clause beyond reach of the most natural common-law challenge.[14] the doctrine remains available in theory. Its practical scope has been substantially narrowed.

V. What the Regulators Are Doing About It

A. The European Framework: GDPR

The EU's GDPR is the most substantive regulatory intervention to date. In force since May 2018, it sets a consent standard that is directly incompatible with the techniques described above. Under Article 4(11), consent must be freely given, specific, informed, and expressed through an unambiguous affirmative act. Pre-ticked boxes don't count. Neither does silence. Neither does inaction. The European Data Protection Board went further, ruling that cookie walls interfaces that condition service access on accepting behavioural tracking cannot satisfy the freely given requirement, because a user whose only alternative is being excluded is not really choosing.

Enforcement has been meaningful. The Irish Data Protection Commission fined Meta €1.2

billion in 2023 for unlawful EU-to-US data transfers. France's CNIL fined Google €150 million in 2022 for a cookie consent interface that collapsed refusal into multiple steps while acceptance required only one click. These are real sanctions, even if they remain small relative to the revenues involved.

B. The United States: CCPA, CPRA, and the FTC

The US picture is more fragmented. Federal legislation on data privacy has stalled for years, leaving the field to state-level statutes. California's CCPA and its successor, the CPRA, have gone furthest giving Californians rights to access, delete, and opt out of data sales, and establishing the California Privacy Protection Agency as a dedicated enforcement body.[19] At the federal level, the FTC's September 2022 report on dark patterns was a useful diagnostic exercise, documenting manipulative practices across hundreds of sites and confirming that they fall within the FTC Act's prohibition on deceptive practices.[20] That framing matters legally. But without a comprehensive federal statute, the impact is inevitably uneven.

C. India: The Digital Personal Data Protection Act 2023

India's DPDPA 2023 takes a different approach, directly addressing the language problem.[21] Consent notices must be in plain language and in the data principal's preferred language. The Act also requires that withdrawal of consent be as simple as giving it in the first place a direct repudiation of the asymmetric interfaces Amazon and others have deployed. Whether these provisions change anything in practice is not yet clear. The Act's implementing bodies are still being constituted. The gap between what the text requires and what Indian platforms currently do is significant, and closing it will depend heavily on how the regulator chooses to use its powers.

VI. Big Tech in the Spotlight

Meta offers a well-documented case study. The company has revised its privacy architecture repeatedly over the years, and each version has tended to default toward maximum data collection. The clearest illustration of the consent problem is the 2014 emotional contagion study, in which the platform systematically altered the content shown to roughly 700,000 users to observe the effect on their subsequent emotional expression.[22] When the study became public, Meta's response was that users had consented through the platform's data use policy.

Technically, this was arguable the policy contained a general research clause. But no reasonable person would have understood, on signing up, that they had authorised their emotional state to be experimentally manipulated. The legal argument worked; the consent argument did not.

Google's location tracking settlement USD 391.5 million, agreed with the attorneys general of 40 states in November 2022 arose from a simpler kind of deception.[23] the company's settings interface included a toggle labelled 'Location History.' Turning it off did not stop location tracking. That continued under a separate setting called 'Web and App Activity,' a label that gave users no reason to think it had anything to do with geography. The design created a false sense of control. Users who thought they had opted out had not.

Amazon's Prime subscription cancellation flow is the cleanest example of deliberate interface asymmetry currently before US courts. The FTC's 2023 complaint documents an internal design process in which the cancellation path called the 'Iliad Flow' by Amazon's own engineers was progressively made more complicated over successive iterations while the sign-up path remained quick and easy.[24] the significance of the case is not just that Amazon is being sued. It is that the complaint frames the asymmetric design itself as a consumer protection violation not a policy question, not a design preference, but an unlawful commercial practice. That framing, if it holds up, has implications well beyond Amazon.

VII. The Ethical Dimension: When Legal Compliance Is Not Enough

Legal compliance analysis of dark patterns tends to stop at the same place: is this practice technically within the rules? That is the wrong question, or at least not the only question. The lawyers who structure and draft digital consumer agreements are not passive transcribers of their clients' instructions. They make substantive choices about how long a document needs to be, where to position a particular clause, how opaque the language should be. Those choices have direct consequences for whether the person who clicks Accept has any real understanding of what they are agreeing to. Calling these choices professional judgments is accurate. That is exactly the point: professional judgments carry professional obligations.

Autonomous decision-making the ability to make real choices based on real information is not just a contract law concept. It underlies informed consent in medical ethics. It grounds the right to self-determination in constitutional jurisprudence. A contractual structure deliberately

designed to prevent the other party from understanding what they're agreeing to is not merely deficient under contract law. It works against the purposes that law is supposed to advance. That observation applies to regulators and courts. It also applies to the lawyers who build these instruments.

VIII. What Reform Should Look Like

A. Mandatory Plain Language Requirements

Insurance policies and consumer credit agreements in many jurisdictions are already subject to plain language requirements. There is no good reason why platform terms of service are not. The objection that detailed legal terms need complex legal language collapses once you note that the same lawyers produce both impenetrable consumer agreements and clear institutional documentation. A plain language mandate would not prevent platforms from maintaining detailed terms for commercial and compliance purposes. It would require, in addition, a version that an ordinary person can actually read. That is not a high bar.

B. Standardised Disclosure Frameworks

Ben-Shahar and Schneider's critique of mandated disclosure is well taken: simply requiring more information does not reliably improve consumer decision-making.[25] but the answer to that finding is better-designed disclosure, not none at all. A standardised, machine-readable summary covering data categories collected, processing purposes, third-party recipients, opt-out paths, and deletion procedures, in a fixed comparable format across all consumer-facing platforms would serve two purposes at once. It would give users who do engage something structured enough to navigate. And it would create an auditable record that enforcement bodies can use to verify compliance without relying solely on user complaints.

C. Judicial Recalibration

The tools courts need already exist. Unconscionability and good faith are not new doctrines. What has been missing is the willingness to apply them to the actual conditions of digital contracting rather than to a stylised picture in which both parties are on equal footing and exit is always available. Courts need to ask not just whether the terms were technically accessible, but whether they were presented in a way that gave the other party any realistic chance of understanding them. That shift does not require legislation. It requires a change in how courts

approach the evidence before them.

D. Meaningful Enforcement and Professional Responsibility

A fine that a major platform absorbs as a cost of doing business is not a deterrent it is a licence fee. Effective enforcement means penalties tied to the commercial benefit derived from non-compliance, not to a fixed statutory cap that becomes irrelevant at sufficient scale. Alongside this, bar associations and law societies should develop guidance specific to consumer digital contracting. The question of what professional responsibility requires when a lawyer's drafting choices are specifically designed to prevent the other party from understanding what they are agreeing to is not one that existing codes of conduct address directly. It should be.

IX. Conclusion

The contractual infrastructure of the digital economy is built on a fiction, and a fairly transparent one. The documents that are said to record users' agreement are not read. The language in them is not understood. The consent they purport to evidence does not, in any meaningful sense, occur. The legal system has accommodated this by insisting on two propositions: that making terms technically available is the same as giving someone a genuine opportunity to understand them, and that clicking a button is a voluntary act of contractual commitment. Neither proposition survives honest scrutiny.

Availability and comprehensibility are different things. Clicking a button without understanding what you're clicking on is not the consent that contract law has historically required. The regulatory direction of travel affirmative and specific consent requirements, sanctions for asymmetric design, plain language mandates, meaningful withdrawal rights reflect a growing acknowledgment that consent must be more than a recorded gesture. Translating that acknowledgment into a coherent legal framework, consistently applied across jurisdictions, is the work that remains.

An agreement that extracts a click from someone who doesn't know what they're agreeing to, written in language designed to prevent understanding, surrounded by interface choices engineered to produce that click, is not a contract in any sense the tradition would recognise. It is a legal label attached to an act of inattention. Calling it consent does not make it consent. At some point, the law has to say so.

References

1. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & Pol'y Info. Soc'y 540 (2008).

2. Harry Brignull, *Dark Patterns: The Dirty Tricks Designers Use to Make You Do Things*, 90 Percent of Everything (Aug. 2010), http://www.90percentofeverything.com.

3. Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies (Harvard University Press 2018).

4. Philipp Lorenz-Spreen et al., *Boosting People's Ability to Detect Microtargeted Advertising*, 11 Sci. Reps. 1 (2021).

5. Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet*, 23 Info. Comm. & Soc'y 128 (2020).

6. Florian Schaub et al., *A Design Space for Effective Privacy Notices*, Soups 2015 Proc. 1 (2015).

7. Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print?*, 43 J. Legal Stud. 1 (2014).

8. Florencia Marotta-Wurgler, *Will Increased Disclosure Help?*, 78 U. Chi. L. Rev. 165 (2012).

9. *Specht v. Netscape Commc'ns Corp.*, 306 F.3d 17 (2d Cir. 2002).

10. *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171 (9th Cir. 2014).

11. *Meyer v. Uber Technologies, Inc.*, 868 F.3d 66 (2d Cir. 2017).

12. *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996).

13. Arthur A. Leff, *Unconscionability and the Code*, 115 U. Pa. L. Rev. 485 (1967).

14. *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333 (2011).

15. Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

16. Eur. Data Prot. Bd., Guidelines 05/2020 on Consent Under Regulation 2016/679 (2020).

17. Data Protection Commission (Ireland), Decision in Case IN-22-5-1 (Meta Platforms Ireland Limited) (May 22, 2023).

18. CNIL, Délibération SAN-2022-022 (Jan. 21, 2022) (Google LLC).

19. California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199; California Privacy Rights Act of 2020.

20. Fed. Trade Comm'n, Bringing Dark Patterns to Light (2022).

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

22. Adam D.I. Kramer, Jamie E. Guillory & Jeffrey T. Hancock, *Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks*, 111 PNAS 8788 (2014).

23. Office of the Attorney General, Multistate Settlement with Google LLC (Nov. 14, 2022).

24. *Federal Trade Commission v. Amazon.com, Inc.*, No. 2:23-cv-00932 (W.D. Wash. filed June 21, 2023).

25. Omri Ben-Shahar & Carl E. Schneider, More Than You Wanted to Know: The Failure of Mandated Disclosure (Princeton University Press 2014).