

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 3

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

The Price of Convenience: Flaws in the Notice-Consent Framework in E-Commerce and Fintech

PRERNA SAHU* AND OENDRI PAL**

ABSTRACT

This paper examines how participation in modern e-commerce and FinTech ecosystems is increasingly conditioned upon the continuous disclosure of personal data as the price of access to services such as retail, payments, credit and financial inclusion. Drawing on Shoshana Zuboff's account of surveillance capitalism, it argues that consent has been rendered largely illusory, as digital platforms have shifted from collecting data as a by-product of service delivery to extracting behavioural data as a core economic resource for prediction, profiling and behavioural influence. It contends that consent fatigue is not merely a consequence of complex digital architecture but a deliberate exploitation of users' cognitive overload, dark patterns and asymmetric power relations, operating disproportionately against economically and digitally marginalised groups. Through a comparative analysis of the European Union's General Data Protection Regulation, India's Digital Personal Data Protection Act, 2023 and landmark judicial precedents from Indian, European and German courts, the paper identifies critical regulatory lacunae in both e-commerce and FinTech. Grounding its normative argument in Kantian and Rawlsian philosophy, it proposes a shift towards a more duty-based regulatory framework and the reconceptualisation of personal data as an extension of selfhood rather than a tradeable commodity.

Keywords: *Surveillance capitalism, Informed consent, Data protection, Consent fatigue, Dark patterns, E-commerce, FinTech, Digital Personal Data Protection Act, GDPR, Data autonomy.*

I. INTRODUCTION

The architecture of the modern digital economy is built on a foundational paradox: the services that citizens rely upon for everyday commerce, credit and financial access are offered freely, yet their true price is the permanent and pervasive surrender of personal data. Consent, the legal mechanism designed to govern this exchange, has become a procedural ritual, omnipresent in

* Author is a student at NMIMS School of Law, Bengaluru, Karnataka, India.

** Author is a student at NMIMS School of Law, Bengaluru, Karnataka, India.

form but hollow in substance. From cookie banners on e-commerce platforms to multi-page privacy disclosures embedded within FinTech loan applications, the act of agreeing has been systematically stripped of the voluntariness that gives it moral and legal force.

This paper addresses a research gap that existing scholarship has identified but not sufficiently pursued in the Indian regulatory context: the structural incompatibility between consent-based data protection frameworks and the behavioural manipulation economy that operates downstream of that consent. Employing a doctrinal and comparative legal methodology, the paper first situates the problem within the theory of surveillance capitalism and interrogates the legal fiction of informed consent under the Digital Personal Data Protection Act, 2023 and the General Data Protection Regulation. It then analyses the mechanics of data aggregation and profiling, examines the ethical dimensions through Kantian and Rawlsian frameworks and connects them directly to reform imperatives. Finally, it proposes concrete pathways for reform.

II. DATA AS CAPITAL: THE RISE OF SURVEILLANCE-DRIVEN BUSINESS MODELS

Online participation increasingly demands that individuals reveal almost all of their personal information, not by choice but as a condition of access to fundamental services in retail, payment systems, credit and financial inclusion.¹ From browsing merchandise on online shopping websites to seeking instant online loans, the process of obtaining consent has become obligatory through constant requests that are legally voluntary but practically impossible to resist. This produces a rift between theory and reality. In the context of the growing phenomenon of surveillance capitalism, the principal legislation governing the manner and means of data use offers only a limited safeguard through the mechanism of informed consent.

Surveillance capitalism marks a transition from the collection of data as a by-product of service delivery to the extraction of data as the principal economic activity of online platforms. In this model, user data is treated as a commodity.² As Shoshana Zuboff describes it, the business model of surveillance capitalism involves the use of behavioural surplus to create predictive products that enable platforms not only to forecast but also to influence the behaviour of their users for monetary benefit.³ This distinction is significant, because conventional data protection regulations were not designed to control the manipulation of behaviour.

In online markets, surveillance capitalism is realised through personalised recommendations, dynamic pricing and online advertisements designed through the continuous tracking of

¹ Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013).

² Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710 (2017).

³ SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER* (Profile Books 2019).

browsing and purchasing behaviour, extending even to the speed of browsing.⁴ In FinTech, these models are even more consequential, as transaction histories, mobile metadata, location and device-level information are used to construct credit profiles for lending and insurance, which are often a prerequisite for accessing vital financial services.

The regulatory framework of data protection, in particular consent-based regimes such as the Digital Personal Data Protection Act, 2023⁵ in India and the General Data Protection Regulation⁶ in the European Union, rests on the notion that users retain effective control over their data through the principle of informed consent. This assumption has become increasingly dubious in light of the role of surveillance. The conflict lies in the fact that the prediction and control of behaviour occurs after the point of click-through consent, well after the agree button has been clicked, so that consent is ineffective in regulating the actual extent of data use. The matter therefore reveals the ingrained paradox between the present reality of online business and traditional notions enshrined in law, where consent is portrayed as little more than a formality.

III. THE LEGAL FICTION OF INFORMED CONSENT

Informed consent remains the foundational model of modern data protection law and an essential cornerstone upon which personal data is processed. Section 6(1) of the Digital Personal Data Protection Act, 2023 provides that consent must be free, specific, informed, unconditional and unambiguous, communicated through a clear affirmative action. Similarly, Articles 4(11), 6(1)(a) and 7 of the General Data Protection Regulation, the governing instrument for data protection in the European Union, stipulate that consent must be freely given, specific, informed and unambiguous, subject to conditions ensuring that the consent obtained is valid. Both regimes are based on the assumption that an individual is enabled to assert control over personal information by making an informed choice.

Informed consent has, however, failed the test of reality within the digital economy and has thus become a legal fiction. Long and complex privacy policies, coupled with the indispensable nature of online platforms, make it almost impossible for individuals to give consent while exercising genuine autonomy. Although data protection law in India continues to depend

⁴ NORWEGIAN CONSUMER COUNCIL, *DECEIVED BY DESIGN: HOW TECH COMPANIES USE DARK PATTERNS TO DISCOURAGE US FROM EXERCISING OUR RIGHTS* (2018).

⁵ The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

⁶ Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.

heavily on consent as the principal justifying factor in the processing of data, it fails to address the imbalance in the power structure between users and platform markets.

Consent interfaces on e-commerce platforms, such as cookie banners or consent pop-ups, tend to bundle permissions and overload users with information, leaving no realistic choice but to consent. This has produced what is increasingly termed consent fatigue.⁷ On major Indian e-commerce platforms such as Flipkart and Meesho, consent interfaces bundle multiple permissions, for advertising, analytics, location tracking and third-party data sharing, into a single click framed as the condition of access. The alternative to consenting is platform exclusion, which for many users engaged in essential commerce is not a realistic option. Consent fatigue is thus not a design failure but a design choice.

In FinTech implementations, the giving of consent is not an option but the price of entry into the services. The privacy notices framed to seek consent are normally couched in technical legal jargon and structured so as to obscure the actual extent of data sharing, retention and secondary use, thereby undermining the purpose of informed consent.

Indian privacy jurisprudence, in particular *Justice K.S. Puttaswamy (Retd.) v. Union of India*,⁸ has located the right to informational privacy in the notions of dignity and autonomy, thereby repudiating consent mechanisms that are formal but devoid of actual choice. This concern is becoming increasingly pertinent in the context of data extraction through platform technologies. The legal framework continues to treat consent as formally valid even when it is practically unavoidable, revealing a gap between statutory ideals and regulatory practice. The Digital Personal Data Protection Act, 2023⁹ reaffirms that consent is the principal legal ground for processing, but it does not provide effective instruments for addressing the imbalance between data principals and data fiduciaries in conditions of platform dominance. For instance, Sections 6(7), 6(8) and 6(9) of the Act introduce Consent Managers, a distinct and heavily regulated category of intermediary intended to act as an agent on behalf of the data principal. Rather than a company setting up its own standard cookie banner or preference centre, a Consent Manager is an independent entity registered with the Data Protection Board of India.¹⁰ However, the Act does not require data fiduciaries to integrate with Consent Managers. A company may bypass them entirely and handle consent in-house through standard pop-ups. Moreover, a Consent Manager may itself centralise consent fatigue. If it presents hundreds of complex privacy

⁷ ZUBOFF, *supra* note 3.

⁸ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

⁹ The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

¹⁰ The Data Protection Board of India is constituted under Chapter V of the Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

notices on a single screen, most users are likely to accept them without reading, rendering the mechanism an operational bottleneck rather than an instrument of genuine agency. Informed consent thus becomes a legal fiction, satisfying the formality of procedural legality while meeting none of the standards required to protect substantive autonomy.

IV. THE MECHANICS OF SURVEILLANCE: DATA AGGREGATION AND PROFILING

Surveillance capitalism is fuelled by the permanent, real-time collection of data that extends well beyond the discrete, specific use of data in transactions ordinarily contemplated at the time of consent. On modern e-commerce platforms, tracking is conducted through cookies, software development kits, device fingerprinting and cross-platform tracking, which together enable the construction of profiles based on user behaviour. In the FinTech sector, algorithmic profiling is more invasive and more significant, because financial risk analysis increasingly relies on non-traditional sources of data such as mobile activity, social interactions and transaction metadata. Such constant aggregation enables platforms to infer information about users that has never been explicitly shared,¹¹ raising serious questions about the extent of the processing.

In *Anuradha Bhasin v. Union of India*,¹² the Supreme Court affirmed the principles of proportionality and necessity in limiting the fundamental rights of citizens, which raises the question why the same principles do not apply to private companies engaged in pervasive data collection. The Court similarly emphasised transparency as a criterion for legitimacy in *Swapnil Tripathi v. Supreme Court of India*,¹³ illustrating the autonomy deficit created by non-transparent algorithmic arrangements on online platforms.

In international contexts, considerable precedent has stressed that such data retention and continuous profiling constitute a serious violation of privacy rights. In *Digital Rights Ireland Ltd. v. Minister for Communications*,¹⁴ the Court of Justice of the European Union held that indiscriminate data retention infringes fundamental rights and confirmed that endless profiling cannot be justified by initial consent. Similarly, the European Court of Human Rights in *S. and Marper v. United Kingdom*¹⁵ acknowledged the psychological harm done to individuals when their data is retained even where it is not used. This concern is highly pertinent to behavioural profiling conducted in the digital sphere.

¹¹ FRANK PASQUALE, *THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION* (Harvard Univ. Press 2015).

¹² *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (India).

¹³ *Swapnil Tripathi v. Supreme Court of India*, (2018) 10 SCC 639 (India).

¹⁴ *Digital Rights Ireland Ltd. v. Minister for Communications*, Joined Cases C-293/12 & C-594/12, ECLI:EU:C:2014:238 (Apr. 8, 2014).

¹⁵ *S. and Marper v. United Kingdom*, App. Nos. 30562/04 & 30566/04, Eur. Ct. H.R. (2008).

From a legal perspective, this thins the foundations of consent-driven regulation, because it is impossible for users of these services to foresee or control the subsequent uses of their data even where consent has been obtained. The persistence and opacity of algorithmic profiling make it evident that the harm caused by surveillance capitalism depends not merely on overt data collection but on what the resulting knowledge asymmetry reveals about disparities in power.

V. ETHICAL AND STRUCTURAL IMPACTS ON USER AUTONOMY

The evolving ecosystem of e-commerce platforms and the FinTech industry, moving from passive observation to intentional manipulation, represents a paradigm shift that challenges the foundations of individual freedom and constitutes a fundamental attack on user autonomy. Under the Kantian categorical imperative, persons should always be treated as ends in themselves and never merely as means to an end.¹⁶ In the surveillance capitalism model, the e-commerce platform treats the user as a data mine, that is, as a mere means to an end. A platform that deploys dark patterns to exploit the psychological state of the user overrides the user's rational decision-making process. The user thereby becomes a predictable biological mechanism, stripped of the dignity that Immanuel Kant identified as the defining quality of moral agents.¹⁷

Moreover, applying John Rawls' theory of justice,¹⁸ and in particular the veil of ignorance, injustices appear at a fundamental level. An equitable society would not permit digital architecture to operate to the detriment of the less privileged. Predatory FinTech nudges and discriminatory lending are typically aimed at those with lower levels of financial literacy or in economically precarious circumstances. These services use non-traditional data such as social media traces, battery levels or typing speed to establish creditworthiness, thereby perpetuating a digital underclass, contrary to Rawls' principle that social and economic inequalities are to be arranged so as to confer the greatest benefit on the least advantaged.

E-commerce addiction loops, specifically designed to trigger dopamine responses, and discriminatory FinTech lending that operates within an algorithmic black box together create a state of digital serfdom. When a human bank manager denies a loan, a reason must be given. When a machine learning model whose internal design is opaque denies it, the response is often that the computer says no, leaving the individual with no means to challenge the decision or

¹⁶ IMMANUEL KANT, *GROUNDWORK OF THE METAPHYSICS OF MORALS* (Mary Gregor trans., Cambridge Univ. Press 1996).

¹⁷ A. Kumar, *Kant on the Ground of Human Dignity*, 26 KANTIAN REV. 435 (2021).

¹⁸ JOHN RAWLS, *A THEORY OF JUSTICE* (rev. ed., Harvard Univ. Press 1999).

correct the underlying data. Where a user's choices are predetermined by an algorithm, freedom of choice becomes illusory.

VI. COMPARATIVE REGULATORY GAPS IN E-COMMERCE AND FINTECH ECOSYSTEMS

Purpose limitation is emphasised in the European Union's General Data Protection Regulation.¹⁹ Under that Regulation, personal data collected for a specific purpose must not be put to any other use without fresh consent being sought. In the Indian context, the Digital Personal Data Protection Act, 2023²⁰ introduces the notion of the data fiduciary, defined as any person who alone or in conjunction with other persons determines the purpose and means of the processing of personal data,²¹ but it grants the Government significant exemptions. Furthermore, it provides no safeguards against the dark patterns that produce consent fatigue.

In *Meta Platforms Inc. v. Bundeskartellamt*,²² the Court of Justice of the European Union, on a reference from the German courts, addressed the prohibition imposed on Meta against merging user data across Facebook, WhatsApp and Instagram without consent. The decision connected antitrust law with data privacy, demonstrating how the latter undermines consumer choice.

In *Google LLC v. Competition Commission of India*,²³ the role of market dominance in creating a structural barrier to free consent was further illustrated. The National Company Law Appellate Tribunal upheld the Competition Commission of India's assessment that Google's dominance in the Android market allowed it to use the Mobile Application Distribution Agreement to require the pre-installation of the entire Google Mobile Suite as a condition of access to the Play Store. This amounts to forced defaultism, which exploits status quo bias and erodes buyer power. The consequence is that the procurement of consent becomes mandatory to the extent that consent is no longer a voluntary manifestation of autonomy but a contract of adhesion to participate in the internet.

VII. PATHWAYS FOR REFORM: RESTORING MEANINGFUL CONSENT AND AUTONOMY

Platforms should be prohibited from collecting data that is not strictly necessary for the primary function of the application. FinTech companies should be required to submit their artificial

¹⁹ General Data Protection Regulation art. 5(1)(b), 2016 O.J. (L 119) 1.

²⁰ The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

²¹ The Digital Personal Data Protection Act, 2023, § 2(i), No. 22, Acts of Parliament, 2023 (India).

²² *Meta Platforms Inc. v. Bundeskartellamt*, Case C-252/21, ECLI:EU:C:2023:537 (July 4, 2023).

²³ *Google LLC v. Competition Commission of India*, Competition Appeal (AT) No. 1 of 2023, 2023 SCC OnLine NCLAT 147 (India).

intelligence models for independent bias audits to prevent discriminatory lending. Privacy should be the default setting, so that users must opt in to behavioural tracking rather than navigate complex menus to opt out.

The judiciary needs to abandon its formalistic approach to consent in favour of a substantive one. In *Data Protection Commissioner v. Facebook Ireland Ltd. and Schrems*,²⁴ the Court of Justice of the European Union struck down the validity of the EU-US Privacy Shield, holding that data protection should follow the data. That precedent supports a principle of extraterritorial autonomy, ensuring that a right is not undermined merely because data is processed outside the territory in which it was collected.

The Digital Personal Data Protection Act, 2023 should be amended to include a duty of care for data fiduciaries. If a FinTech platform's nudges lead a user into a debt trap through manipulative interface design, the platform should be held liable for breach of fiduciary duty.

VIII. CONCLUSION

With the rise of the digital economy, personal data has become a resource ripe for exploitation, exposing the inadequacies of current consent-based mechanisms of data protection. As discussed above, surveillance capitalism operates through the constant extraction of personal data, algorithmic profiling and power asymmetries that may render the principle of informed consent meaningless. Within e-commerce and FinTech, consent becomes a means of gaining access to systems rather than a genuine choice, thereby infringing the principles of respect, privacy and self-determination that data protection provisions are intended to safeguard.

Addressing this problem requires a move from procedure towards substance. Stricter duties of data minimisation, algorithmic transparency and fiduciary care are needed to rebalance the relationship between platforms and individuals. Ultimately, data must be recognised not only as a commodity but also as an extension of personhood, deserving of legal protection.

²⁴ *Data Protection Commissioner v. Facebook Ireland Ltd. and Schrems* (Schrems II), Case C-311/18, ECLI:EU:C:2020:559 (July 16, 2020).