Page 1568 - 1577 **DOI:** *https://doij.org/10.10000/IJLMH.1111425*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 1

2026

Consent Centrism in Targeted Advertising: Structural Threat to Informational Self Determination

VERSHIKA SHARMA[1]

ABSTRACT

Targeted advertising is one of the less discussed topics within legal analysis and and even lesser known are the legal harms inscribed within the structural framework of targeted advertising. This article first conceptualizes targeted advertising within the legal framework of informational self determination and then critically analyses the structural irregularities in the adequacy of consent centrism in tackling them. The notice and consent mechanism evolved in the DPDPA does not adequately prevent constitutional harms amidst existence of high knowledge and power asymmetries in modern digital market place. The article then delves into a comparative analysis of the multilayered consent framework of the GDPR and its efficacy in solving persisting legal problems under the DPDPA. The DPDPA essentially relies almost completely on consent for legitimising data processing particularly in the absence of strong supervisory mechanisms. However, under the GDPR, consent is not the sole legitimising principle for data processing rather it functions within a broader framework of multiplicity of doctrines, principles and supervising and oversight authorities to provide holistic rights based approach and reducing risk burden on users by reducing reliance on consent mechanism. The article argues that users are in no position to meaningfully consent in structural market asymmetries, thereby lack of other ex ante measures under the DPDPA must be revised as a way forward.

Keywords: *privacy, dpdpa, gdpr, targeted advertising, informational self-determination*

I. INTRODUCTION

The modern digital marketplace is founded on an inherent contradiction unbeknownst to a common user. The general perception is that the internet is freely available. But this is inaccurate as there is a clear value exchange where the users pay in the form of personal data.[2] The digital economy is highly reliant on extraction and analysis of user's personal data for monetisation through various means and one prevalent method is targeted advertising.[3]

[1] Author is a Research Scholar at Rajiv Gandhi National University of Law, Patiala, India.
[2] Lina M Khan, 'Amazon's Antitrust Paradox' (2017) 126 *Yale Law Journal* 710, 745–746.
[3] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019) 8–12.

 [ISSN 2581-5369]

Often, the users remain in the blind spot to meaningfully consent to any kind of data mining owing to prevalent information asymmetries, take-it-or-leave-it consent models, lack of awareness, complex and long privacy policies etc.[4] This widespread data collection has the potential to violate informational self-determination which now warrants constitutional protection in India.[5] The system functions on the model of surveillance capitalism where the data collection and analysis is persistent across the platforms, learning browsing habits, location history, content engagements and other actions across the internet into behavioral profiles harnessed through AI, machine learning and algorithmic analysis.[6]

This provides a "personalised" character to advertisements that are behaviorally targeted utilising advanced technology.[7] These advertisements have been defended on the basis of convenience and improved user experience while privacy harms caused due to underlying and back end processes are brushed under the carpet.[8] Therefore, instead of questioning legitimacy in light of violation of constitutional principles of informational self determination, the convenience logic purports to normalise continuous and deeply pervasive targeted advertising practices.[9] The justification for such widespread data processing is often rooted in the notice and consent model.[10] This model essentially mandates data collecting and processing entities to inform users about it for obtaining informed and meaningful consent.[11] However, there is growing concern about the adequacy and efficacy of the consent framework in light of systematically devised core structures of modern digital markets to escape liability.

This article takes this argument forward to highlight the inherent contradictions in targeted advertising which encompasses both commercial convenience and legal anomalies. The major concern beyond covert manipulation relies on sophisticated structurally inbuilt mechanisms of converting user footprint on the internet into behavioral profiles to drive commercial profits without user knowledge. This article acknowledges the advantages of targeted advertising but tests the same on the touchstone of fundamental right to privacy. To this effect, the article critically examines the existing legal framework of informational privacy enforced through the notice-and-consent model of data protection and its efficacy in governance of targeted

[4] Frederik Zuiderveen Borgesius, *Improving Privacy Protection in the Area of Behavioural Targeting* (Kluwer Law International 2015) 21–25.
[5] *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 pp [298], [307], [312] (*Puttaswamy I*).
[6] Zuboff (n 2).
[7] Ibid.
[8] Avi Goldfarb and Catherine Tucker, 'Privacy and Innovation' (2012) 12 Innovation Policy and the Economy 65.
[9] Julie E Cohen, *Between Truth and Power* (OUP 2019) 55–60.
[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ L119/1 (GDPR) arts 4(11), 6(1)(a), 7; Digital Personal Data Protection Act 2023 (India) s 6.
[11] Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harv L Rev 1880.

 [ISSN 2581-5369]

advertising. The legal analysis is limited to the notice-and-and consent framework to holistically address the encompassing nuances of notice-and-consent in governance of targeted advertising amidst ever growing concerns around its efficacy.

II. UNDERSTANDING TARGETED ADVERTISEMENT WITHIN CONSENT FRAMEWORK

There is no legal framework which has categorically defined targeted advertising till date. However, many scholars have devised effective definitions of targeted advertising to include collection and analysis of large volumes of personal data across the internet. This data is collected through browsing history, cookies, Software development kits, applications, pixels etc.[12] The processing occurs through machine learning, AI, automated and semi automated processes.[13] This collection and analysis of data culminates into creation of predictive and behavioral profiles of users which can sometimes include sensitive information.[14] Once user profiles are created, targeted advertisements are delivered based on inferred preferences.[15] For instance, an advertisement for Nike shoes valued INR 10,000 will be delivered to users whose profile might reveal inclination for frequent interaction with sports shoes, Nike, purchasing power of INR 10000, running affinity and other similar details.

One prominent real world example of targeted advertising is Real Time Bidding (RTB). This means publication of advertisement within seconds of bidding in the auction for advertising space on a relevant website and includes sharing personal information with advertising intermediaries to connect them with potential buyers.[16] For instance, a user clicks on the hindu article on travel destinations in India. Immediately, the website opens it for instant auctions and companies like Make My trip, GoIbibo etc. rush to make a bid realising your interest in travelling and by default hotels. The advertisement of highest bidder is published within the timeframe that the page takes in loading. Both the abovementioned examples demonstrate that with or without user awareness, their data almost always circulates across the internet to cater to targeted advertising and allied processes.[17]

III. TARGETED ADVERTISEMENT AND THE INFORMATIONAL SELF-DETERMINATION

The legal discourse on informational self determination started in the German constitutional

[12] Borgesius (n 3) 45–52.
[13] Zuboff (n 2) 94-97.
[14] Ibid.
[15] Ibid.
[16] Johnny Ryan, 'Behavioural Advertising and Personal Data' (2019) 1–3.
[17] Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (2014).

 [ISSN 2581-5369]

court. According to the court, informational self-determination means complete authority over one's own personal information be it offline or online and encapsulates control over how this information is used, processed and analysed.[18] The same principle is reiterated by the Indian judiciary in *Justice KS Puttaswamy (Retd) v Union of India* (2017).[19] The apex court stated that "*Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the State but from non-State actors as well… The ability of an individual to control the dissemination of personal information is an essential facet of informational privacy.*"[20] Therefore, the judicial position in India regarding informational privacy is clear – it is protected under part III of the Indian Constitution.

The intersection of targeted advertising and informational self-determination occurs at the instance the user loses control over his/her personal information when it is collected, processed and analyzed for behavioral profiling standing at the core of targeted advertising without consent. The advocates of targeted advertising argue that personal data when obtained and processed with user's consent does not violate informational self determination under privacy.[21] Usually, consent clauses are embedded in the detailed and complex privacy policies often bundled with other terms and conditions. Assent to these privacy terms and conditions is a prerequisite to access the platforms. Research clearly demonstrates that users hardly ever read the entire policies and if they do, comprehension is an additional burden.[22] Therefore, the action of ticking terms and conditions boxes is more of a procedural formality rather than an exercise of valid and meaningful consent.[23]

Meaningful consent requires meaningful information. The opacity of processes involved in behavioral profiling defies access to this meaningful information. This occurs in the instances of clearly defining the "what" and "how" of personal information. This clarity is lost in the huge volumes of degraded quality of information available for making decisions of acceptance of privacy policies. These policies run into thousands of words in addition to already long cookie policies.[24] This huge volume renders these policies practically unreadable in the absence of simplified and shorter versions. Secondly, there are concerns regarding the quality of available information. For instance, phrases like "personal information can be used to improve the quality

[18] Bundesverfassungsgericht (Federal Constitutional Court) 15 December 1983, 65 BVerfGE 1 (Census Act Case).
[19] *Justice K.S. Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 (SC) [248].
[20] Ibid [190].
[21] Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679* (17/EN WP259 rev.01) 13-15.
[22] Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harv L Rev 1880.
[23] Zuboff (n 2) 48-52.
[24] Ben-Shahar and Schneider, *More Than You Wanted to Know* (Princeton University Press 2014) 3–12.

 [ISSN 2581-5369]

of our server"[25] or "the user information may be stored for as long as needed"[26] are vague and embedded with uncertainty of current and future use of personal information.[27] This increases the risk of plausible abuse of information especially in the absence of "what" and "how" the information will be used, processed and repurposed and for how long. Lastly, there is a lack of information alternatives rendering ultimate dependence on available information from the corporation the only source of information.[28] The verifiability of all available information is questionable for lack of supervisory and auditing agencies.

Therefore, in the absence of appropriate, efficient and adequate information about collection, storage and processing of personal data, there is no real control over one's own data. This renders the opaque processes involved in targeted advertising subject to constitutional scrutiny under violation of informational self determination.

Sensitive attributes inferred from publicly available private information

The inferences drawn from data driven and algorithmically analysed behavioral profiling further complicate matters. Although, any kind of sensitive information is generally protected against targeted advertisement across jurisdictions including India.[29] However, when sensitive inferences are derived and predicted from publicly accessible information about an individual, such as sexual and political inclinations, health and fitness related attributes etc., it triggers legal uncertainty because these algorithmic inferences deviate from traditional definitions of sensitive information.[30] Consequently, they may not be granted automatic protection available to the conventional categories of personal data.[31] For example, a user engages with pages advocating for LGBTQ+ rights, pride parades, queer groups and influencers etc. This information is clearly "public" but the user has not publicly claimed to belong to this category explicitly across any platform. However, the highly complex algorithmic analysis aggregates small actions across

[25] Meta Platforms Inc, *Privacy Policy* https://www.facebook.com/privacy/policy accessed 17 January 2026 (screenshot taken 12 January 2025).
[26] Ibid.
[27] Neil Richards and Woodrow Hartzog, 'The Pathologies of Digital Consent' (2019) 96 *Washington University Law Review* 1461, 1463.
[28] Ibid.
[29] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, arts 9(1)–(2) (prohibiting processing of special categories of personal data, including for profiling and advertising, unless specific conditions such as explicit consent are met); Digital Personal Data Protection Act 2023 (India) ss 6(1), 9 (requiring explicit consent for processing of children's data and restricting behavioural tracking and targeted advertising directed at children); see also Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, r 3 (defining 'sensitive personal data or information' and restricting its disclosure without consent).
[30] Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2 *Columbia Business Law Review* 494.
[31] Ibid.

 [ISSN 2581-5369]

the internet to infer a user's connection with the community, by belonging or supporting.[32] This information is highly sensitive and may carry political undernote which requires heightened protection.

When the algorithm assigns certain meaning to user's online engagements through specific inferences, the user loses control over the meaning assigned to their online behavior along with data. The ability to have control over data includes the ability to control its interpretation as well.[33] In the example above, the user may have simply exercised curiosity or academic engagement which may have algorithmically be interpreted as association or sexual identity. This (mis)interpretation is later used to categorize and demarcate for profiling, targeting and other market related activities. Although, outside the scope of this article, it is imperative to acknowledge the social and political harms arising out of stigma associated with certain categories particularly due to unauthorised information disclosure. This may also lead to political messaging, price and opportunities related discrimination, unwarranted exposure to hostile content etc.[34]

Secondly, assuming that the algorithm correctly interprets the sexual orientation of the individual through their online engagements, it creates an opportunity for platforms to use and sell highly sensitive information without consent. The user loses control not only over the interpretation but also on what sensitive attribute of their personality is being shared or sold, to whom and when, all of which should be controlled explicitly by the data owner.[35] The person may not want to be contextually categorised as "obese" or "likely obese" simply to cater to advertising convenience. This context collapses in targeted advertising, where social content engagements become advertising profiles, public self expression becomes data and curiosity leads to classification is a direct threat to user autonomy, self expression, dignity and privacy.[36]

The user has absolutely no control over the repurposing and secondary use for lack of transparency, awareness and comprehension of the sheer volume of individual data used for predictive analytics rendering is practically impossible for users to have any control over. Therefore, this sensitive inferences from publicly available non-sensitive information warrants heightened protection at par with primary sensitive information under the applicable laws.

---

[32] Ibid.
[33] Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019) 83–92
[34] Oscar H. Gandy, Jr., *The Panoptic Sort: A Political Economy of Personal Information*(2nd edn, Oxford University Press 2021)
[35] Watcher (n 29).
[36] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2010).

 [ISSN 2581-5369]

IV. LIMITATIONS OF NOTICE-AND-CONSENT FRAMEWORK IN GOVERNING TARGETED ADVERTISING

The systematic framework of information collection and predictive analysis for targeted advertising is almost entirely reliant on consent doctrine for legitimacy. The same is reflected deeply under the global data protection regime and reiterated in the Indian Digital Personal Data Protection Act, 2023 (DPDPA) and the Digital Personal Data Protection Rules, 2025 (DPDP Rules). This article delves deeper into the consent framework under DPDPA and GDPR to critically analyse the efficacy of consent centrism in protecting informational self determination.

Consent as Legitimizing Doctrine for Data Mining Under Indian DPDPA

Consent has been established as the basic mandate for processing personal information under the DPDPA. It follows the rights based approach of GDPR wherein consent must be "free, unambiguous, certain, specific and unconditional" to be sought through "clear and intelligible" notice.[37]

The notice provisions under DPDPA requires consent seeking notices to include details regarding all data that will be collected and processed along with clear purpose along with rights of the user in plain and clear language.[38] These rights should clearly specify the right of withdrawal without adverse consequences and manner of such withdrawal along with the complaint mechanism.[39] The requirements are operationalised under DPDP Rules which mandate the notice to be clear, self contained and "understandable independently" of other documents along with item description purpose(s).[40] One unique feature of the Indian legal framework on data protection is "consent managers" that are registered intermediaries involved in review and withdrawal of consent with ease.[41]

For consent to be valid under DPDPA, it must be "free, specific, informed, unconditional and unambiguous" and for a "specific purpose."[42] The act itself expounds upon purpose specification by limiting consent to only "personal data necessary for that specified purpose."[43] The user is also given the right to withdraw consent completely or partially at any time with

[37] Digital Personal Data Protection Act 2023 (India) ss 5(1)–(3), 6(1) (DPDPA).
[38] Digital Personal Data Protection Act 2023 (India) s 5.
[39] Ibid.
[40] *Digital Personal Data Protection Rules, 2025*, Rule 3.
[41] Ibid Rule 4.
[42] DPDPA s 6(1).
[43] Ibid.

 [ISSN 2581-5369]

ease at par with which consent was given.[44]

Consent as ONE of the Legitimising basis for processing personal data under GDPR: A Comparative Analysis

Consent is treated as a lawful basis for data processing under the GDPR but is *not* the only basis.[45] Rather, consent is seen as more of an operationalising instrument of the principle of self-determination but in no way taking away from the broader foundational regulatory framework of accountability, purpose limitation, necessity, legitimate public interest and protection of user rights.[46] This reverberates scholarly scepticism towards adequacy and universality of consent centrism in ensuring appropriate safeguards against data driven market structures which shift the burden of risk assessment and reduction on users inefficient in market asymmetries leading to consent paradox.[47]

As with the DPDPA, consent under GDPR must be "freely given, specific, informed and unambiguous" through a "clear and affirmative act."[48] There are relevant clarifications regarding these requirements. Consent will not be automatically considered "free" dynamics where there is information and power asymmetries.[49] For instance, when there is employability at stake and when consent is reliant on accessibility to the platform as a precondition. This is one key difference between the doctrinal jurisprudence in India and under the GDPR as this additional interpretative recital supports that there is a possibility of structural coercion masked under the garb of formal agreement.

There is also heightened protection with explicit consent in cases of sensitive information.[50] These additional safeguards account for added layers of protection creating accountability in cases of hidden coercion, bundled assents and even structural asymmetries. Additionally, the responsibility to show that consent was lawfully obtained relies on the controller which must be obtained separately and clearly along with easy withdrawals.[51] Therefore, consent is not merely a passive acquiescence fulfilling formal contractual obligation rather it is now a clear, active and demonstrable authorisation based in operationalisation of informational self

[44] Ibid s 6(4).
[45] Regulation (EU) 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] OJ L119/1 (GDPR), art 6(1)(a).
[46] Bundesverfassungsgericht (German Federal Constitutional Court) *Census Act Case* (Volkszählungsurteil) BVerfGE 65, 1 (1983).
[47] Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019).
[48] GDPR (n 37), art 4(11).
[49] Ibid recital 43.
[50] Ibid art 9.
[51] Ibid art 7.

 [ISSN 2581-5369]

determination through transparency. Consequently, there has been adequate emphasis by regulators that data controllers and intermediaries follow lawful processing as a precondition and not an afterthought to remedy unlawful profiling retrospectively.[52] The GDPR essentially uses consent as a legitimising tool for exercise of fundamental rights along with a broader regulatory framework for balancing risk burden.

The DPDPA endorses a seemingly similar approach to legitimize data processing through a consent centric approach for exercising informational self determination by adopting similar validity mandates. The adaptation of purpose limitation and data minimisation doctrines along with easy withdrawal setup requirements provide some depth into the consent framework.[53] However, consent within the GDPR does not replace an additional well established regulatory framework of data protection. For instance, the DPDPA fails to address the structural imbalance deeply embedded within data processing frameworks that manifests in the form of information and power asymmetries which may render consent bereft of meaning. This can occur in the contexts where there is platform dominance, infrastructural indispensability, conditioned service accessibility, opaque and unnecessary data processing or even economic dependence which can only be addressed through ex ante regulatory measures. Therefore, consent centrism warrants extra scrutiny in markets dominated by behavioral profiling and targeted advertising.

The GDPR endorses a stronger audit and supervisory mechanism adopting a multilayered monitoring and oversight mechanism.[54] The DPDPA, on the other hand, has opted for a more centralised and executive heavy Data Protection Board which has been criticised for possibility of bias in cases involving the State and powerful private entities specially in the absence of independent supervisory bodies unlike the GDPR.[55] Secondly, unlike the GDPR, the Indian data protection board lacks powers to take suo motto cognisance, conduct proactive audits and enact binding guidelines (particularly in the absence of a qualified interpretative body).[56] This, coupled with the possibility of political pressure on the regulator, could weaken enforcement in structurally established targeted advertising market frameworks.

In conclusion, while there is substantive doctrinal overlap between DPDPA and the GDPR

[52] European Data Protection Board, *Guidelines 05/2020 on Consent under Regulation 2016/679* (Version 1.1, adopted 4 May 2020).
[53] GDPR (n 37) ss 5, 6(1), 6(4).
[54] Ibid arts 51–63.
[55] Gautam Bhatia, 'The DPDP Act and the Architecture of Executive Control' (2023) *Indian Constitutional Law and Philosophy* (2023); see also Aashi Dixit, 'Data Protection in India after the Digital Personal Data Protection Act, 2023: A Critical Evaluation of Privacy and State Power' (2026) 6 *Indian Journal of Legal Review* 116, 116–130.
[56] Aashi Dixit, 'Data Protection in India after the Digital Personal Data Protection Act, 2023: A Critical Evaluation of Privacy and State Power' (2026) 6 *Indian Journal of Legal Review* 116, 116–130.

 [ISSN 2581-5369]

regarding consent as a legitimising mechanism, there is significant divergence with respect to deeper regulatory constraints, independent supervision and substantive consent framework. The risks are highly exacerbated in the more complex matrix of behavioral profiling and targeted advertising marred with pronounced asymmetries and which occur after crossing the peremptory gatekeepers.

V. THE WAY FORWARD

There is a need for structural accountability in the Indian data protection regime moving away from extreme consent centrism. This would ideally encompass regulatory reforms in the DPDPA to include an independent supervisory body. This must include industry experts to meaningfully analyze cases and provide binding guidelines as is the case with the GDPR. The body must have auditing and suo motto powers to take cognisance of matters proactively within the ambit of provisory guidelines but without unnecessary procedural delays. Regular audits of Significant Data Fiduciaries must be included as a mandate for this overseeing body to impose accountability on those who handle large volumes of personal data.

On a doctrinal level, there is a need to imbibe structural asymmetries within the consent framework lest it is rendered entirely ineffective. This article does not deny the utility of consent based framework in enforcement of exercise of basic rights such as autonomy, dignity, privacy and informational self determination. However, consent needs to be meaningful which is less probable if the current information and power asymmetries remain intact. Users neither have the means nor the technical prowess to uncover layers of complex processes involved in targeted advertising. The only way to bring meaning into consent is through balancing the asymmetries to the extent possible which can happen through ex ante regulatory measures. Consent framework, by itself will always fail here. The need is to supplement it with ex ante impact assessment, bring more transparency into algorithmic processing, and stronger rules for sensitive data along with vulnerable groups. This would enhance platform accountability, regulatory oversight and independent supervision all of which would provide better starting ground for implementation of exercise of meaningful decision making while giving consent for data processing.

*****

 [ISSN 2581-5369]