Convergence of Competition Law and Constitutional Rights: A Comparative Study of the WhatsApp (India) and Facebook (Germany) Cases

by

Anush Ganesh[*]
Krusha Bhatt[**]

CONTENTS

I. Introduction
II. Comparative Case Study: WhatsApp's Privacy Policies
  1. The 2021 WhatsApp Privacy Policy Update
  2. The Indian Enforcement Action
  3. Regulatory Responses in the EU
  4. Comparative Insights
III. Theoretical Foundations: Constitutional Rights and Consumer Protection
  1. The Indian Constitutional Approach
  2. The EU Approach
  3. Converging Foundations

[*] Anush Ganesh, Postdoctoral Research Fellow at the University of Exeter (United Kingdom); email: anush.ganesh@stmarys.ac.uk; ORCID: https://orcid.org/0009-0003-3940-1725.

[**] Krusha Bhatt, Lecturer, Jindal Global Law School (India); email: kbhatt@jgu.edu.in; ORCID: https://orcid.org/0000-0001-8426-4633.

Suggested citation: Anush Ganesh, Krusha Bhatt, 'Convergence of Competition Law and Constitutional Rights: A Comparative Study of the WhatsApp (India) and Facebook (Germany) Cases' (2025) 18(31) YARS.

Article received 12.05.2025, accepted 22.10.2025.

Yearbook of Antitrust and Regulatory Studies, Vol. 18, No. 31, pp. 131–154 • ISSN 1689-9024
https://doi.org/10.7172/1689-9024.YARS.2025.18.31.10

IV. Methodological Approaches: Integrating Competition Law with Other Legal Regimes
1. The Indian Integrative Approach
2. The European Institutional Cooperation Approach
3. Comparative Assessment
V. Toward a Unified Framework for Assessing Excessive Data Collection
1. A Four-Part Test for Assessing Exploitative Data Practices
2. Institutional and Remedial Implementation
VI. Conclusion: Implications for Global Platform Regulation

Abstract

As society advances toward a digital economy with increasing dependence on internet-based services, data has attained prominence as an essential currency supporting market power. This paper examines the emerging jurisprudence on excessive data collection by dominant digital platforms, comparing approaches developed in India and the European Union. The Indian approach, exemplified by the WhatsApp Privacy (2025) decision, integrates competition law with constitutional protections, particularly the right to privacy under Article 21 of the Indian Constitution. Meanwhile, the European approach, crystallized in the Facebook Germany case, integrates competition law with data protection principles enshrined in the General Data Protection Regulation (GDPR). Despite their different legal foundations, these approaches display convergence in recognizing that dominant platforms' data collection practices can constitute abusive exploitation of market power. This paper argues that this convergence creates opportunities for a unified analytical framework that respects jurisdictional diversity while enabling more effective global platform regulation.

Resumé

À mesure que la société évolue vers une économie numérique de plus en plus dépendante des services Internet, les données ont pris une importance considérable en tant que monnaie essentielle soutenant le pouvoir de marché. Cet article examine la jurisprudence émergente relative à la collecte excessive de données par les plateformes numériques dominantes, en comparant les approches développées en Inde et dans l'Union européenne. L'approche indienne, illustrée par la décision WhatsApp Privacy (2025), intègre le droit de la concurrence aux protections constitutionnelles, en particulier le droit à la vie privée prévu à l'article 21 de la Constitution indienne. Quant à l'approche européenne, cristallisée dans l'affaire Facebook Allemagne, elle intègre le droit de la concurrence aux principes de protection des données consacrés par le règlement général sur la protection des données (RGPD). Malgré leurs fondements juridiques différents, ces approches convergent en reconnaissant que les pratiques de collecte de données des plateformes dominantes peuvent constituer une exploitation abusive du pouvoir de marché. Cet article soutient que

cette convergence crée des opportunités pour un cadre analytique unifié qui respecte la diversité juridictionnelle tout en permettant une réglementation mondiale plus efficace des plateformes.

Key words: Competition, Data, Abuse of dominance, 102, CCI, India, Germany.

JEL: K21

I. Introduction

As society advances toward the creation of a digital economy and intensifies its dependence on internet-based services, we are producing increasingly meaningful digital footprints both passively and actively. In the digital economy age, data has attained the prominence of an essential currency supporting the architecture of market power.[1] The proliferation of digital platforms has fundamentally transformed the relationship between businesses and consumers, creating novel challenges for traditional regulatory frameworks.[2]

Platforms like WhatsApp and Facebook (now Meta) occupy positions of unprecedented influence, controlling essential communication infrastructure while operating under 'zero-price' business models that monetize user data rather than charging direct fees.[3] However, the characterization of these services as 'free' obscures a more complex transaction where consumers exchange personal data for platform access, often without meaningful comprehension of the value being transferred or the implications of such exchange.[4] The case against leading technological platforms such as WhatsApp and Facebook, now part of the Meta group, increasingly focuses on how they utilize vast amounts of data to enhance their market position, customize services for individual consumers, and generate economic advantages often at the expense of consumer autonomy.[5]

---

[1] Nicholas Economides and Ioannis Lianos, 'Restrictions on Privacy and Exploitation in the Digital Economy: A Market Failure Approach' (2021) 17(4) Journal of Competition Law & Economics 765.

[2] Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition Policy for the Digital Era – Final Report' (2019) European Commission, 19–24.

[3] John M Newman, 'Antitrust in Zero-Price Markets: Foundations' (2015) 164 University of Pennsylvania Law Review 149.

[4] Anush Ganesh, 'Pricing Practices in Digital Markets: An Abuse of Dominance Approach' (PhD thesis, University of East Anglia School of Law, 2022), https://ueaeprints.uea.ac.uk/id/eprint/94200/, 102–103.

[5] David S Evans, 'Attention Platforms, the Value of Content, and Public Policy' (2019) 54 Review of Industrial Organization 775.

While traditional competition law analyses have historically focused on factors such as pricing, barriers to market entry, and market exclusion, contemporary scholarship emphasizes the imperative of reevaluating aspects related to the exploitation of dominance within the framework of data-driven business models.[6] This paper examines the emerging jurisprudence on excessive data collection by dominant digital platforms, comparing approaches developed in India and the European Union.

The Indian approach, exemplified by the *WhatsApp Privacy* (2025) decision of the National Company Law Appellate Tribunal (NCLAT), integrates competition law with constitutional protections, particularly the right to privacy under Article 21 of the Indian Constitution.[7] Meanwhile, the European approach, crystallized in the *Facebook Germany* case,[8] integrates competition law with data protection principles, particularly those enshrined in the General Data Protection Regulation (GDPR).[9]

Despite their different legal foundations, these approaches display convergence in recognizing that dominant platforms' data collection practices can constitute abusive exploitation of market power. This paper argues that this convergence creates opportunities for a unified analytical framework that respects jurisdictional diversity while enabling more effective global platform regulation.

The paper is structured as follows: Section 2 examines the theoretical foundations of both approaches, comparing the constitutional rights-based framework in India with the consumer protection orientation in Europe. Section 3 analyzes the methodological approaches to integrating competition law with other legal regimes. Section 4 conducts a comparative case study of enforcement actions against WhatsApp's privacy policies in both jurisdictions. Section 5 proposes a unified framework for assessing excessive data collection that draws on both approaches. Section 6 concludes with implications for global platform regulation.

---

[6] See Crémer et al. (n 2).

[7] *WhatsApp LLC v Competition Commission of India & Ors* [2025] NCLAT I.A No. 280 of 2025 in Competition App. (AT) No. 1 of 2025.

[8] Case C-252/21, *Meta Platforms v Bundeskartellamt*, EU:C:2023:537.

[9] Ibid.

II. Comparative Case Study: WhatsApp's Privacy Policies

1. The 2021 WhatsApp Privacy Policy Update

In January 2021, WhatsApp announced a significant update to its privacy policy that would require users to consent to expanded data sharing between WhatsApp and other Meta-owned platforms.[10] The privacy policy enacted in 2021 fundamentally rendered it obligatory for users to consent to the sharing of their data, which is collected through WhatsApp, with all affiliated Meta companies.[11] Key changes included:

- Mandatory sharing of WhatsApp user data with other Meta companies
- Expansion of data collected, including device-level information and usage patterns
- A 'take-it-or-leave-it' approach requiring acceptance to continue using the service
- Vague and open-ended language regarding future data uses

These changes triggered regulatory scrutiny in multiple jurisdictions, most prominently in India and the European Union, providing an opportunity to compare different regulatory approaches to essentially identical platform behaviour.

2. The Indian Enforcement Action

The CCI took *suo motu* cognizance of WhatsApp's 2021 privacy policy update, finding that WhatsApp abused its dominant position in the Indian market for Over-The-Top (OTT) messaging apps by imposing unfair conditions on users.[12] The CCI's analysis focused on several key elements:

First, the CCI found WhatsApp to be dominant in the Over-The-Top (OTT) messaging market, with a market share of approximately 90% based on Daily Active Users. The Director General during its investigation found WhatsApp to be dominant in the market for OTT messaging Apps in India.[13] As of 2022 survey by Statista, in relation to the ten most frequently used messaging services in India based on Daily Active Users (DAU) and Monthly

[10] WhatsApp Privacy Policy (04 January 2021) https://www.whatsapp.com/legal/privacy-policy.

[11] *Re: Updated Terms of Service and Privacy Policy for WhatsApp users*, Suo Motu Case No. 01 of 2021, para 164.1

[12] Ibid. paras 41 and 130.

[13] Ibid. para 42.

Active Users (MAU), 90% users ranked WhatsApp, and 56% users ranked Messenger (by Meta) as their most preferred messaging service.[14]

Second, the CCI determined that the 'take-it-or-leave-it' nature of the policy constituted an abuse under Section 4 of the Competition Act.[15] Unlike previous policy updates, the 2021 policy provided no opt-out option, effectively requiring users to consent to data sharing to continue using the service. The CCI agreed with the investigation conducted by the DG which determined that the WhatsApp 2021 privacy update does not provide an option to opt-out.[16] Unlike its 2016 and 2019 policy updates,[17] end users are not voluntarily consenting to the dissemination of their personal information.[18]

Third, the CCI found WhatsApp's data collection excessive, particularly due to the 'vague, broad and open-ended' language and the lack of an exhaustive list for the kinds and purposes of data collected.[19] The absence of transparency 'inhibits users from engaging in well-informed decision-making processes' and positions them unfavourably, as they cannot fully understand the magnitude of data being collected and shared.[20]

Finally, the CCI connected the excessive data collection to competitive harm, noting that platforms can leverage their extensive data repositories to create barriers to entry, exclude competitors, or engage in discriminatory practices, thus stifling competition and reducing consumer welfare in the long run.[21] The consolidation of data from diverse origins equips Meta with analytical insights that smaller rivals are unable to duplicate, potentially obstructing the entry of new competitors and consolidating market dominance in favour of established entities.[22]

The CCI issued a cease-and-desist[23] order and imposed significant monetary penalty of 213.14 crore rupees[24] on WhatsApp for abusing its dominant position in the OTT market in violation of section 4 of Indian Competition Act by imposing unfair conditions[25], creating entry barriers denying market access[26] to its competitors in the market for online display advertisement and leveraging

[14] Ibid. para 72.
[15] Ibid. para 166.
[16] Ibid. para 183.
[17] Ibid. para 135.1.
[18] Ibid. para 136.
[19] Ibid. para 166.
[20] Ibid. para 167.
[21] Ibid. para 28.3.
[22] Ibid. para 182.3.
[23] Ibid. para 246.
[24] Ibid. para 263.
[25] Section 4(2)(i) of the Competition Act, 2002.
[26] Section 4(2)(c) of the Competition Act, 2002.

its dominant position in the OTT market for strengthening its position in the online display advertisement market in India.[27] The NCLAT subsequently upheld this decision, affirming the CCI's jurisdiction and analysis.[28]

When platforms control essential communication, commerce, and information services, their data collection policies become quasi-governmental decisions about surveillance, economic access, and social participation. The 'take-it-or-leave-it' nature of these policies, combined with the lack of meaningful alternatives,[29] transforms private terms of service into systems of social control that warrant constitutional scrutiny.

In the Indian context, the emphasis on substantive equality provides tools for addressing the infrastructural dimension that enables platforms to engage in data collection practices that only have the aim of entrenchment of their dominant position. When data collection policies systematically disadvantage vulnerable populations or enable discriminatory treatment,[30] they violate constitutional equality principles regardless of their formal neutrality. The EU's consumer protection approach addresses similar concerns in their unique manner which can provide useful insights to assessment of data collection practices by dominant digital platforms.[31]

3. Regulatory Responses in the EU

While not specifically addressing the 2021 WhatsApp update, the *Facebook Germany* case established precedent that would influence European approaches to similar privacy policy changes as seen previously.[32] Beyond the *Facebook* case, the 2021 WhatsApp privacy policy update[33] triggered regulatory responses in Europe. The European Data Protection Board coordinated an investigation by Ireland's Data Protection Commission.[34]

---

[27] Section 4(2)(e) of the Competition Act, 2002.

[28] *WhatsApp LLC v. Competition Commission of India* I.A No. 280 of 2025.

[29] *WhatsApp privacy policy* 2021 (n 74) para 166.

[30] Katharine Kemp, 'Concealed data practices and competition law: why privacy matter' (2020) 16(2) European Competition Journal 628, 653.

[31] See Ganesh Doctoral thesis (n 4) 97–138.

[32] Bundeskartellamt *Facebook* Decision (n 36) para 914.

[33] *WhatsApp 2021 Privacy Policy* (n 74).

[34] Data Protection Commission, In the matter of WhatsApp Ireland Limited (DPC Inquiry Reference: IN-18-12-2) (Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act 2018 and Articles 60 and 65 of the General Data Protection Regulation, 20 August 2021).

The Data Protection Commission's landmark investigation resulted in a record €225 million fine for WhatsApp's failure to meet transparency obligations under Articles 12–14 of the GDPR, establishing that tech companies must provide information in a concise, transparent, intelligible and easily accessible form. This penalty represented the second-largest GDPR fine at that time, surpassed only by Amazon's €746 million fine.[35]

Despite WhatsApp's claims that the fine was disproportionate, the regulatory action forced meaningful changes to protect European users' privacy rights.[36] WhatsApp was compelled to rewrite its European privacy policy, adding substantial detail about data collection, usage, storage, deletion practices, and cross-border data sharing mechanisms. This case illustrates that financial penalties coupled with mandated policy revisions can effectively bring even the largest tech companies into compliance with European data protection standards, providing a template for future regulatory interventions.

4. Comparative Insights

Despite functioning within fundamentally divergent legal paradigms- India rooted in common law traditions and Germany in civil law- the regulatory approaches of India and Europe towards platform supremacy and data exploitation reveal a significant convergence. This alignment is particularly evident in the regulatory reactions to the activities of digital behemoths such as Meta and WhatsApp, which, while operating as subsidiaries within the same corporate conglomerate, are nonetheless subjected to jurisdiction-specific oversight. The investigation launched by the Competition Commission of India (CCI) in 2021 concerning WhatsApp's revised privacy policy, alongside the 2019 ruling from the German Federal Cartel Office (FCO) against Facebook's data collection methodologies, represent pivotal moments in this international convergence.

Both authorities recognized that dominant digital platforms are uniquely positioned to impose terms on users in a "take-it-or-leave-it" fashion. In the *WhatsApp 2021 Privacy Policy* case, the CCI took *suo motu* cognizance of the policy's unilateral imposition, noting that users had "no meaningful choice" but to accept data sharing with Facebook or lose access to the service entirely. This echoed the reasoning of the German FCO in its decision against Facebook (Meta), where the court found that users were compelled to agree

[35] Damian Graham, 'WhatsApp updates privacy policy after record €225 million fine' (Euronews, 22 November 2021) https://www.euronews.com/next/2021/11/22/whatsapp-rewrites-its-europe-privacy-policy-after-a-record-225-million-gdpr-fine.

[36] Ibid.

to the extensive tracking of their behaviour across third-party websites and apps, even when not using Facebook's core services.

In both cases, the imbalance of market power and the dependency of users on these platforms formed the basis for competition concerns, linking privacy intrusions directly to market dominance.

The Indian CCI should connect WhatsApp's data practices to the constitutional right to privacy as recognized in *Justice K.S. Puttaswamy (Retd.) v Union of India*. The CCI must emphasize that antitrust enforcement cannot be divorced from fundamental rights where data is concerned, given that excessive data collection directly affects informational self-determination. Similarly, the German decision situated its analysis within the framework of the General Data Protection Regulation (GDPR), arguing that data collection which violates user consent norms also undermines competitive fairness. Here, competition law was applied in tandem with data protection regulation, thereby acknowledging user autonomy as both a privacy and competition concern.

A common thread in both cases is the concern about whether the extent of data collection was proportionate to the business objective pursued.[37] The German FCO held that Facebook's practice of merging user data from various sources (including Instagram and WhatsApp) without explicit consent was not just a privacy violation but an abuse of dominance.[38] This closely parallels the CCI's assessment of WhatsApp's policy as an opaque and involuntary mechanism for cross-platform data harvesting by Meta, without offering users a granular opt-out. By invoking proportionality, both decisions resonate with the *Puttaswamy* ratio, especially its emphasis on legitimacy, necessity, and minimal impairment of rights.

Both the Indian and German regulatory bodies recognized that excessive data extraction does not merely harm individual users but also distorts competition. The CCI warned that Meta's access to WhatsApp data could be leveraged to consolidate power across markets reducing contestability. Similarly, the German FCO found that Facebook's super-profile creation entrenched its position by reinforcing network effects and raising barriers to entry. Thus, privacy exploitation and anticompetitive behaviour were viewed as mutually reinforcing the exploitation of users feeds into the exclusion of competitors.

This convergence suggests the emergence of a common understanding of platform dominance and its relationship to data practices that transcends jurisdictional boundaries especially pertaining to the users' rights to informational privacy.

---

[37] Marco Botta and Klaus Wiedemann, 'Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision', (2019) 10(8) Journal of European Competition Law & Practice 465.

[38] See Section 2.2 of the paper.

III. Theoretical Foundations: Constitutional Rights and Consumer Protection

1. The Indian Constitutional Approach

In the digital ecosystem of India, prevailing social media platforms such as WhatsApp exert substantial social infrastructural authority over communication, commerce, and personal identity.[39] The concerns regarding the privacy policy of WhatsApp are not a novel phenomenon in India. Previously, analogous objections were raised against the revision of its privacy policy in 2016 before the Delhi High Court.[40] The Delhi High Court, nonetheless, abstained from addressing the argument pertaining to the right to privacy in relation to the amendments instituted by the 2016 update, rationalizing that the determination of the right to privacy as a fundamental right remains to be adjudicated by the Supreme Court and also that fundamental rights cannot be exercised against non-state actors.[41]

The Court in 2016 privacy policy matter concluded that user data collected through WhatsApp should be erased for individuals whose accounts were deleted prior to September 25, 2016, and this data will not be shared further. Conversely, for those users who opt to continue utilizing WhatsApp services, the data accrued subsequent to September 25, 2016, was subjected to sharing with third party.[42] This practically means that for availing WhatsApp services, a user must consent to the updated privacy policy or delete their account. The Delhi high court decision is reflective of dire need to have appropriate laws and governing bodies around consumer data protection in India. Absence of which is costing privacy of the Indian users.

With a significant turning point in 2017, the Indian approach to regulating dominant platforms' data practices is anchored in constitutional rights jurisprudence, particularly the landmark judgment in *Justice K.S. Puttaswamy v Union of India*.[43] In *Puttaswamy*, the Supreme Court recognized privacy as a fundamental right protected under Article 21[44] of the Indian Constitution, with informational privacy as a key dimension of this right which "protects the

[39] India Social Media Statistics 2025 | Most Used Popular Top Platforms. (2025). https://www.theglobalstatistics.com/india-social-media-statistics/

[40] *Karmanya Singh Sareen and Anr v Union Of India And Ors* W.P.(C) 7663/2016 & C.M.No.31553/2016.

[41] Ibid. paras 17–18.

[42] Ibid. para 20.

[43] *Justice K.S. Puttaswamy (Retd.) and Another v Union of India and Others* (2017) 10 SCC 1

[44] Protection of life and personal liberty.

inner sphere of the individual from interference from both State, and non-State actors and allows the individuals to make autonomous life choices."[45]

In Indian constitutional law the application of fundamental rights first between private parties corresponds to horizontal application, while the application between individuals and the State corresponds to vertical application. Although the Indian Constitution was originally designed for fundamental rights to apply vertically (Article 12[46] of the Indian Constitution), Indian courts have slowly expanded horizontal application in certain contexts. Throughout the years, the interpretation of "State" as delineated in Article 12 of the Constitution has experienced substantial transformation.[47] The Supreme Court in *Vishaka v. State of Rajasthan (1997)*[48] curated guidelines for preventing sexual harassment at workplace binding even on private employers in conformity with the fundamental rights as enshrined under Articles 14[49], 15[50], 19(1)(g)[51] and 21[52] of the Indian Constitution.

On Page 264 of the *Puttaswamy* judgment, the Court held:

> "*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.*"[53]

Under the current anti-trust regulatory scheme in India, the Competition Commission of India (CCI) and the National Company Law Appellate Tribunal (NCLAT) are the competent bodies that can extend this constitutional analysis to the competition realm, recognizing that dominant platforms like WhatsApp perform quasi-public functions that justify the horizontal application of fundamental rights. This approach does not merely view WhatsApp's privacy practices as a contractual matter between private parties, but as implicating core constitutional values that warrant regulatory intervention. This approach is supported by the reasoning of the Indian Supreme Court in the case of *Zee Telefilms Ltd v Union of India* (2005)[54] where the court while acknowledging

---

[45] *Justice K.S. Puttaswamy* case (n 14) per Kaul J., para 77.

[46] "The State" includes the Government and Parliament of India and the Government and the Legislature of each of the States and all local or other authorities within the territory of India or under the control of the Government of India.

[47] *Pradeep Kumar Biswas v Indian Institute of Chemical Biology* (2002) 5 SCC 111*; Zee Telefilms Ltd. v Union of India*, (2005) 4 SCC 649; *Janet Jeyapaul v. S.R.M. University* (2015) 16 SCC 530.

[48] *Vishaka & Ors v State of Rajasthan & Ors* AIR 1997 SUPREME COURT 3011.

[49] Equality before law.

[50] Prohibition of discrimination on grounds of religion, race, caste, sex or place of birth.

[51] Right to to practise any profession, or to carry on any occupation, trade or business.

[52] Protection of life and personal liberty.

[53] *Justice K.S. Puttaswamy* case (n 14) per Chandrachud J., p. 264.

[54] *Zee Telefilms Ltd v Union of India* (2005) 4 SCC 649.

private bodies to be classified as "State" under Article 12 when they perform public functions held that, "…when a private body exercises its public functions even if it is not a State, the aggrieved person has a remedy not only under the ordinary law but also under the Constitution, by way of a writ petition under Article 226"[55]

Recently, the Supreme Court of India in the case of *Kaushal Kishore v. State of Uttar Pradesh* (2023)[56] was tasked with the question if the fundamental rights available under Articles 19 and 21 of the Indian Constitution be asserted against bodies other than State or its instrumentalities as under Article 12 of the Indian Constitution. To answer the question the court distinguishing between common law rights and fundamental rights held that "The rights in the realm of common law, which may be similar or identical in their content to the Fundamental Rights under Article 19/21, operate horizontally: However, the Fundamental Rights under Articles 19 and 21, may not be justiciable horizontally before the Constitutional Courts except those rights which have been statutorily recognised and in accordance with the applicable law."[57] Combining the ratio decidendi of the leading decisions in *Zee Telefilms*, *Puttaswamy* and *Kaushal Kishor*, it is to be understood that Indian Constitution does extend fundamental rights horizontally where conduct of the non-state players affect these rights negatively. The extension of the right to privacy in the context of data collection can be found in the *Digital Personal Data Protection Act (DPDPA)*, 2023.[58]

The Supreme Court of India, in the landmark case of *Puttaswamy*, has recognized the right to privacy as a fundamental entitlement secured in Article 21 of the Indian Constitution, consequently also broadening its application which imposes a positive obligation on private entities as well.[59] Although the *Puttaswamy* decision does not directly ponder the horizontal application of the fundamental rights doctrine, several judges of the nine-judge constitutional bench acknowledged that privacy could have horizontal implications.[60]

Holding right to privacy as a fundamental right, Justice Kaul opined that

> "*In an era where there are wide, varied, social and cultural norms and more so in a country like ours which prides itself on its diversity, privacy is one of the most important rights to be protected both against State and non-State actors and be recognized as a fundamental right.*"[61]

[55] Ibid. at para 33.
[56] *Kaushal Kishore v State of Uttar Pradesh* (2023) 8 S.C.R. 581.
[57] Ibid. at para 199.
[58] Digital Personal Data Protection Act 2023, No. 22 of 2023 (India). https://www.dpdpa.in
[59] *Justice K.S. Puttaswamy* case (n 14) per Chandrachud J. at p. 264, para (I).
[60] Ibid. at p. 202, para 142.
[61] *Justice K.S. Puttaswamy* case (n 14) per Kaul J., p. 43 para 79.

The constitutionality of the WhatsApp privacy policies is already under challenge for being violative of right to privacy before the Supreme Court of India.[62] While decision in this matter by the Indian Apex Court is awaited, it is now the time to ponder upon the notion that dominant digital platforms such as WhatsApp ought to be held accountable not only through the economic justifications of competition law but also via the ethical tenets enshrined within the Indian Constitution particularly the right to privacy as delineated in Article 21 of the Indian Constitution. Against the developed background, it is contended that WhatsApp, even though a private entity, provides services that, by their nature, have made it a non-alienable platform for the Indian users. The CCI's assertion of jurisdiction over 2021 WhatsApp's privacy policy was affirmed by both the Delhi High Court[63] and the Supreme Court of India[64], establishing that competition authorities have a legitimate role in addressing data practices that both exploit consumers and distort market competition.

By acknowledging the intersection of antitrust regulations and fundamental human rights in the horizontal layer, Indian regulatory bodies and judicial institutions can cultivate a pro-user-rights competition jurisprudence that embodies both the structural complexities and constitutional ambitions of a digital society.

2. The EU Approach

In contrast to India's constitutional rights orientation, the European approach is more explicitly grounded in consumer protection and data protection frameworks, particularly the GDPR. In the *Facebook Germany* case, the Bundeskartellamt (German Federal Cartel Office – German FCO) determined that Facebook's data collection practices violated the GDPR and constituted an abuse of dominance under Section 19 of the German Competition Act (equivalent to Article 102 TFEU).[65]

In February 2019, the Bundeskartellamt passed a decision prohibiting Facebook/Meta from combining user data from different sources and found it to have abused its dominant position due to the lack of effective consent provided by its users.[66] The decision considered the breach of provisions of the GDPR to amount to an abuse of dominant position under Section 19 GWB

[62] *Karmanya Singh Sareen v Union of India* SLP (C) 804/2017. https://www.scobserver.in/cases/karmanya-singh-sareen-union-of-india-whatsapp-facebook-privacy-case-background/

[63] *WhatsApp LLC v Competition Commission of India* (2022) 293 DLT 616.

[64] *Meta Platforms Inc v Competition Commission of India & Anr* SLP (C) No. 17121/2022.

[65] CJEU Decision *Meta Platforms* (n 8) para 49.

[66] Bundeskartellamt, decision no. B6-22/16 of Feb. 6, 2019.

(German Competition Act) which is the German equivalent of Article 102 TFEU in accordance with Article 3 of Reg. 1/2003.[67]

The German Federal Court of Justice (FCJ) upheld this finding, emphasizing that users must be provided with meaningful choice regarding data sharing and personalization.[68] The FCJ held that users must be provided with a choice when it comes to intensive personalization of the user experience and thereby have autonomy over how much data they wish to part with.[69] The CJEU ultimately confirmed that competition authorities may reference GDPR infringements when assessing abuses of dominance.[70]

The case established that competition authorities could consider breaches of data protection law when evaluating whether a dominant firm's conduct constitutes abuse.[71] This principle was ultimately confirmed by the Court of Justice of the European Union (CJEU), which held that a competition authority may, in the exercise of its powers... take account, as one circumstance among others, of the compatibility of that practice with the provisions of the GDPR.[72]

It has been a point of debate whether unfair pricing or unfair trading conditions provide the more appropriate framework for addressing excessive data collection.[73] This debate reflects broader theoretical questions about how to conceptualize data in competition frameworks traditionally focused on price-based analysis.[74] While data might conceptually be viewed as a 'price' that consumers pay for ostensibly free services, the German FCO characterized Facebook's data collection as imposing 'unfair business terms' rather than an excessive price, noting that 'data is free in the eyes of most users even though it might be considered a currency or commodity by the firm.'[75]

The German FCO noted in its decision that the requirement of processing large amounts of user data for an advertising-funded platform to efficiently run its business model does not outweigh the interests of the consumer and that collecting data outside the sphere of the social network platform went

---

[67] Law against Restraints of Competition (Gesetz gegen Wettbewerbsbeschränkungen – GWB) Ch. 2.

[68] Bundesgerichtshof, The Federal Court of Justice provisionally confirms the allegation of abuse of a dominant position by Facebook, No. 80/2020, KVR 69/19 – decision of June 23, 2020.

[69] Ibid paras 86, 120 and 121.

[70] See CJEU Decision *Meta Platforms* (n 8) para 62.

[71] Ibid. para 63.

[72] Ibid.

[73] Viktoria HSE Robertson, 'Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data' (2019) 57 Common Market Law Review 161.

[74] Anne C. Witt, 'Excessive Data Collection as a Form of Anticompetitive Conduct: The German Facebook Case', (2021) 66(2) The Antitrust Bulletin 276.

[75] See Bundeskartellamt *Facebook* Decision (n 37) para 570.

against consumer interests.[76] The German FCO also noted that the lack of transparency is exacerbated by the existence of market power.[77] Due to the existence of Facebook's dominant position and market power, consumers do not have a chance to provide their consent freely.[78]

3. Converging Foundations

Despite their different starting points, the Indian constitutional and European consumer protection approaches converge around several key principles:

First, both recognize that dominant platforms occupy positions of such significance that traditional notions of 'consent' and 'choice' must be re-examined. The imbalance of power between users and dominant platforms undermines the voluntariness of consent, creating a direct nexus between market power and privacy protection.

Second, both approaches acknowledge that platforms like WhatsApp perform functions that transcend traditional private commercial relationships. The Indian approach frames this explicitly through the concept of 'quasi-public entities,' while the European approach implicitly recognizes this through the concept of 'gatekeepers' in the Digital Markets Act (DMA).[79]

Third, both recognize the importance of informational self-determination-whether framed as a constitutional right (India) or as a data protection principle (EU). This concept becomes the normative foundation for assessing when data collection practices constitute abuse.

This convergence suggests the possibility of a unified theoretical framework that respects jurisdictional diversity while enabling more coordinated global approaches to platform regulation.

The constitutional analysis of platform data collection practices gains empirical grounding from comprehensive research into digital platform pricing behaviors and their relationship to market dominance.[80] Platforms systematically collect user data not merely for service provision, but as inputs

[76] Ibid. para 914.

[77] Ibid. para 963.

[78] Ibid. para 385.

[79] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act); See also Anush Ganesh, Mohit Yadav and Gaurav Pathak, 'The Indian draft digital competition bill and report: a critical perspective' (2025) 9(2) Indian Law Review 193–207.

[80] See Ganesh Doctoral thesis (n 4) 97–138; See also Klaudia Majcher, Coherence between Data Protection and Competition Law in Digital Markets (Oxford University Press 2024).

for sophisticated pricing strategies that can approximate first-degree price discrimination and facilitate predatory pricing through cross-subsidization.[81] In the EU context, Article 102 TFEU can address individual pricing abuses, but struggles to capture the systematic nature of data-enabled exploitation that occurs across multiple markets and consumer interactions simultaneously.[82] This ability to leverage data collection across an entire ecosystem of services distinguishes platform power from traditional market dominance and suggests why constitutional-level intervention becomes necessary.[83]

IV. Methodological Approaches: Integrating Competition Law with Other Legal Regimes

1. The Indian Integrative Approach

The Indian approach integrates competition law with constitutional principles in a direct manner. When the Delhi High Court[84] and Supreme Court[85] affirmed the CCI's jurisdiction over WhatsApp's privacy policy, they effectively endorsed the view that competition authorities can directly consider constitutional values when evaluating exploitative abuses by dominant firms. This integrative approach is grounded in the recognition that the Competition Act itself has constitutional foundations. The genesis of Indian Competition Law can be articulated within the framework of directive principles of state policy as enshrined under Article 39(b)[86] and (c)[87] of the Indian Constitution.[88] Entry 21 of the concurrent list, Schedule VII of the Indian Constitution confers upon the legislature the requisite legislative authority to enact laws governing

---

[81] Anush Ganesh, 'Law and economics of price personalization: relevance of secondary-line injury cases under Article 102(c) TFEU' (2025) European Competition Journal, 1–37, https://doi.org/10.1080/17441056.2025.2499318.

[82] Damian Clifford, Inge Graef and Peggy Valcke, 'Pre-formulated Declarations of Data Subject Consent— Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections', (2019) 20(5) German Law Journal, 679–721.

[83] See Ganesh Doctoral thesis (n 4) 134–138.

[84] *WhatsApp LLC v Competition Commission of India* (2022) 293 DLT 616.

[85] *Meta Platforms Inc v Competition Commission of India & Anr* SLP (C) No. 17121/2022.

[86] The State shall, in particular, direct its policy towards securing that the ownership and control of the material resources of the community are so distributed as best to subserve the common good.

[87] The State shall, in particular, direct its policy towards securing that the operation of the economic system does not result in the concentration of wealth and means of production to the common detriment.

[88] Part IV of the Indian Constitution, 1950. https://www.mea.gov.in/Images/pdf1/Part4.pdf

competition in India.[89] This constitutional grounding legitimizes the CCI's consideration of privacy impacts when assessing abuses of dominance.

The CCI's analysis of WhatsApp's privacy policy emphasized how the lack of transparency is exacerbated by the existence of market power.[90] This establishes a crucial link between dominance and exploitation- WhatsApp's market power enables it to impose data collection terms that users cannot meaningfully reject.

The initial objections posited by WhatsApp, which contended that the Competition Commission of India lacks the requisite jurisdiction to engage with matters pertaining to data and privacy, as this is not a per se antitrust issue, were rejected.[91] Emphasizing the role of competition authorities in the current age where "Data" has become a determining force of competition for the "data-driven enterprises",[92] the CCI in its order noted that, "…platforms can leverage their extensive data repositories to create barriers to entry, exclude competitors, or engage in discriminatory practices, thus stifling competition and reducing consumer welfare in the long run."[93]

2. The European Institutional Cooperation Approach

The European approach emphasizes institutional cooperation between competition authorities and data protection regulators. When the CJEU confirmed that competition authorities could consider GDPR violations, it specified that 'the competent data protection authority within Article 51 GDPR and the competition authority must cooperate sincerely to ensure that obligations laid down in the GDPR are fulfilled.'[94]

This cooperative approach is grounded in Article 4(3) TEU, which requires EU institutions to act in good faith and uphold common EU interests. As Advocate General Rantos noted, 'allowing competition authorities to incidentally examine GDPR related violations while assessing an abuse of dominance case… seems to be one that considers the common goals that all EU institutions are bound by.'[95] The CJEU further clarified that competition

[89] Entry 21 of List III, Schedule VII of the Indian Constitution. https://www.constitutionofindia.net/schedules/list-iii-concurrent-list/

[90] *Re: Updated Terms of Service and Privacy Policy for WhatsApp users*, Suo Motu Case No. 01 of 2021, para 28.5.

[91] Ibid., para 28.

[92] Ibid., para 28.1.

[93] Ibid., para 28.3.

[94] See CJEU Decision *Meta Platforms* (n 7) para 54.

[95] Case C-252/21, *Meta Platforms v Bundeskartellamt*, Opinion of AG Rantos, 20 September 2022 para 33.

authorities are 'bound by the prior decisions of the competent data protection authority while considering a GDPR infringement.'[96] This creates a hierarchical relationship where data protection authorities retain ultimate authority over GDPR interpretation, while competition authorities can incorporate these interpretations into their abuse of dominance analyses.

In September 2022, AG Rantos opined that the Bundeskartellamt in fact did not try to penalise a breach of GDPR, but instead used the non-compliance of an undertaking to its provisions to review a case relating to abuse of dominance.[97] In July 2023, the CJEU answered the referral for a reliminary reference by the Higher Regional Court of Dusseldorf in the case of *Facebook* in Germany by holding that a competition authority may refer to an infringement of the GDPR in the context of an abuse of a dominant position.[98] It further stated that such reference to a breach of the GDPR provisions while determining an abuse under Article 102 TFEU would not be considered replacing the competent date protection authority,[99] but would rather take into consideration the importance of personal data and its processing as a '...significant parameter of competition between undertakings in the digital economy.[100]'

3. Comparative Assessment

The Indian and European approaches represent different methodological solutions to the common challenge of addressing multidimensional harms caused by dominant platforms. The Indian approach favors direct incorporation of constitutional values into competition analysis, while the European approach emphasizes institutional coordination while maintaining distinctions between legal regimes.

Both approaches have strengths and limitations. The Indian approach provides a more unified analytical framework but risks overburdening competition authorities with complex constitutional questions. The European approach maintains clearer institutional boundaries but may create coordination challenges and potential delays. The EU's *Meta*/*Facebook* decision framework provides a template for institutional coordination that constitutional approaches could adapt. The requirement that competition

[96] See CJEU Decision *Meta Platforms* (n 7) para 56.
[97] See AG Rantos Opinion in *Meta* (n 61) para 24.
[98] See CJEU Decision *Meta Platforms* (n 7) para 49.
[99] Ibid. para 50.
[100] Ibid. para 51.

authorities cooperate with data protection authorities while maintaining their distinct competencies offers a model for preserving specialized expertise while enabling comprehensive oversight.[101]

Despite these differences, both approaches recognize that excessive data collection by dominant platforms simultaneously raises competition concerns and implicates other legal values whether constitutional rights (India) or data protection principles (EU). This recognition provides a foundation for developing a more unified analytical framework.

V. Toward a Unified Framework for Assessing Excessive Data Collection

Drawing from both the Indian constitutional and European consumer protection approaches, this section proposes a unified framework for assessing when data collection by dominant platforms constitutes an abuse. This framework integrates constitutional values with competition principles while providing concrete guidance to competition authorities.

Both the Indian and European approaches recognize the limitations of traditional price-based competition analysis when addressing data practices. Platform data collection enables cross-subsidization strategies that can constitute predatory pricing while simultaneously exploiting consumers through excessive data extraction.[102] However, the non-depleting nature of data makes it very different when considered a form of currency and determining the economic value also becomes a complicated procedure as online platforms have vague privacy policies.[103] Instead, both approaches assess the fairness of trading conditions imposed by dominant platforms, avoiding the challenges of quantifying data's value while focusing on the conditions under which data is collected.

A unified framework should move beyond attempts to treat data as a direct analogue to price, instead focusing on a holistic assessment of whether dominant platforms are imposing conditions that undermine informational self-determination.

---

[101] Ibid. para 54.

[102] Anush Ganesh, 'Predatory pricing in platform markets: a modified test for firms within the scope of Article 3 of the DMA and super-dominant platform firms under Article 102 TFEU' (2025) 21(2) European Competition Journal 231–266.

[103] Magali Eben, 'Market Definition and Free Online Services: The Prospect of Personal Data as Price' (2018) 14(2) Journal of Law and Policy for the Information Society 227, 281.

1. A Four-Part Test for Assessing Exploitative Data Practices

Drawing from both approaches, we propose a four-part test that integrates constitutional values and competition principles:

1. Necessity Assessment: Is the data collection necessary for the core functionality of the service?
   This criterion parallels the proportionality analysis in Indian constitutional jurisprudence and the necessity principle in European unfair trading conditions cases. From cases like *SABAM*,[104] *GEMA II*,[105] and *DSD*,[106] conditions may be deemed unfair if they are 'not necessary towards achieving the object of the contract.'[107]
   Competition authorities should assess whether each category of data collected is genuinely necessary for providing the service that users have sought, with the burden of proof resting with the dominant platform.
2. Transparency Evaluation: Has the platform provided clear, specific, and comprehensible information about data collection?
   This reflects the transparency obligations in the GDPR and the concern in both jurisdictions about 'vague, broad and open-ended' privacy policies.[108] The CCI noted that the absence of transparency 'inhibits users from engaging in well-informed decision-making processes.'[109]
   Policies must articulate in plain language what data is collected and for what specific purposes, with vague or open-ended provisions presumptively deemed abusive.
3. Consent Genuineness: Does the platform offer meaningful choice regarding data collection?
   This addresses the 'take-it-or-leave-it' concern central to both the Indian WhatsApp case and the German Facebook case. It recognizes that formal consent may not constitute genuine choice when presented by a dominant platform.
   Competition authorities should consider whether users have granular options regarding data sharing and whether lock-in effects and switching costs constrain their freedom of choice.

---

[104] Case C-127/73, *Belgische Radio en Televisie and société belge des auteurs, Compositeurs et éditeurs v. SV SABAM and NV Fonior*, ECLI:EU:C:1974:25.

[105] *GEMA Statutes Commission Decision* (Case IV/29.971) 82/204/EEC [1982] OJ L94/12.

[106] Case C-385/07 P, *Der Grüne Punkt – Duales System Deutschland GmbH v. Commission*, ECLI:EU:C:2009:456.

[107] See *GEMA* [36].

[108] *Re: Updated Terms of Service and Privacy Policy for WhatsApp users*, Suo Motu Case No. 01 of 2021, para 166.

[109] Ibid. para 167.

4. Proportionality Analysis: Is the value extracted through data collection proportionate to the value provided to users?
   This incorporates the proportionality principle from Indian constitutional jurisprudence and the economic value considerations from European competition law. It requires assessing whether the data collection is justified by the value of services provided to users. Competition authorities should scrutinize data collected for purposes unrelated to service improvement, particularly when data is used to entrench dominance or leverage market power into adjacent markets.

Puttaswamy has developed a similar four-step test based on the principles of legitimacy and proportionality to determine whether the limitation on the right to privacy can be justified.

"(i) The action must be sanctioned by law;
(ii) The proposed action must be necessary in a democratic society for a legitimate aim;
(iii) The extent of such interference must be proportionate to the need for such interference;
(iv) There must be procedural guarantees against abuse of such interference."[110]

This framework mirrors the competition law approach where any interference with user autonomy through data extraction must be legally justified, necessary for a legitimate economic purpose, proportionate, and subject to safeguards.

Here is a table below summarising the framework.

Table 1. Four-Part Test for Assessing Exploitative Data Practices

Test Element	Assessment Criteria	Legal Foundation	Implementation Standard
1. **Necessity Assessment**	Is the data collection necessary for the core functionality of the service?	**Constitutional**: Indian proportionality analysis from *Puttaswamy* **Competition Law**: European unfair trading conditions cases (*SABAM*, *GEMA II*, *DSD*) – conditions unfair if 'not necessary towards achieving the object of the contract'	Burden of proof on dominant platform to demonstrate genuine necessity for each category of data collected Must be directly related to service provision users have sought

[110] *Justice K.S. Puttaswamy* case (n 13) per Chandrachud J., p. 264, para (H).

Table 1. (cont.)

Test Element	Assessment Criteria	Legal Foundation	Implementation Standard
2. **Transparency Evaluation**	Has the platform provided clear, specific, and comprehensible information about data collection?	EU: Transparency obligations under the GDPR India: Vague, broad and open-ended' privacy policies that inhibit users from engaging in well-informed decision-making processes.	Policies must articulate in plain language – 1) what data is collected and 2) For what specific purposes Presumption: Vague or open-ended provisions deemed abusive
3. **Consent Genuineness**	Does the platform offer meaningful choice regarding data collection?	*Puttusamy*: WhatsApp 'take-it-or-leave-it' concerns *Meta*/*Facebook:* formal consent insufficient when presented by dominant platform	Competition authorities must assess whether choice constraints undermine genuine consent
4. **Proportionality Analysis**	Is the value extracted through data collection proportionate to the value provided to users?	Constitutional: Indian proportionality principle from Puttaswamy Competition: EU economic value considerations (*Meta; AKKA*/*LAA*[a])	Scrutinize particularly data collected for purposes unrelated to service improvement and whether such data can be used to entrench dominance

[a] Case C-177/16, *Autortiesību un komunicēšanās konsultāciju aģentūra / Latvijas Autoru apvienība v Konkurences padome* EU:C:2017:689.

2. Institutional and Remedial Implementation

Implementing this unified framework would require institutional arrangements that respect jurisdictional diversity while enabling effective enforcement. The framework's implementation would require domestic coordination mechanisms between competition authorities, data protection agencies, and courts, along with international cooperation arrangements that enable information sharing while respecting constitutional limits. Technical capacity building must provide these institutions with expertise necessary to evaluate complex algorithmic systems and their constitutional implications. Drawing from both approaches, several principles emerge:

First, competition authorities should establish formal mechanisms for cooperation with data protection authorities and consumer protection

agencies, recognizing that each brings complementary expertise to the analysis of platform practices.

However, joint application requires institutional innovations that preserve the integrity of different legal frameworks while enabling coordinated enforcement. An effective approach can be clear allocation of primary authority combined with mandatory consultation and coordination requirements that ensure comprehensive analysis without institutional conflict.[111]

Second, competition authorities should explicitly incorporate proportionality analysis into their assessments of exploitative abuses, drawing from constitutional jurisprudence (India) or unfair trading conditions precedents (EU).

Third, remedies should focus on restoring user autonomy rather than merely imposing fines, with behavioral commitments that address the root causes of exploitation.

Remedies for digital market abuses require ongoing positive obligations rather than simple prohibitions.[112] Data minimization requirements, algorithmic transparency mandates, and interoperability obligations represent the type of affirmative duties that constitutional frameworks traditionally avoid but which prove essential for meaningful platform oversight.[113]

VI. Conclusion: Implications for Global Platform Regulation

This paper has examined how India and the European Union approach the regulation of dominant digital platforms' data collection practices, revealing significant convergence despite different legal traditions. The analysis compared India's constitutional rights-based framework, anchored in the Indian Supreme Court's *Puttaswamy* decision recognizing privacy as a fundamental right, with Europe's consumer protection approach, exemplified by the German *Facebook* case and subsequent CJEU ruling. Through detailed case studies of enforcement actions against WhatsApp's 2021 privacy policy update, the paper demonstrated how both jurisdictions reach similar conclusions about platform accountability through different legal pathways.

---

[111] Filippo Lancieri and Caio Mario da Silva Pereira Neto, 'Designing Remedies for Digital Markets: The Interplay Between Antitrust and Regulation' (2022) 18(3) Journal of Competition Law and Economics 613–669.

[112] Anush Ganesh, 'Effective remedies in digital market abuse of dominance cases' (2025) 21(2) European Competition Journal 371–420.

[113] See Clifford et al. (n 53).

The comparison reveals convergence at three levels. Normatively, both jurisdictions recognize that traditional concepts of consent and market choice require re-examination when applied to dominant platforms controlling essential digital infrastructure. Methodologically, both approaches integrate multiple legal frameworks, acknowledging that platform harms cannot be addressed through single-regime analysis. Institutionally, both jurisdictions are developing specialized enforcement mechanisms that combine traditional competition authority powers with new forms of ongoing oversight.

However, this convergence also reveals persistent challenges. The temporal mismatch between constitutional adjudication and digital market dynamics requires institutional innovations that preserve constitutional authority while enabling adaptive oversight. The expertise gap between constitutional interpretation and technical platform analysis necessitates new forms of collaboration between courts, competition authorities, and specialized technical bodies. The enforcement complexity arising from platforms' global operations demands coordinated international approaches that respect constitutional sovereignty while preventing regulatory circumvention.

To address these challenges, the paper proposed a unified analytical framework consisting of a four-part test for assessing exploitative data practices: necessity assessment, transparency evaluation, consent genuineness, and proportionality analysis. This framework enables competition authorities to incorporate constitutional values without exceeding their institutional competence while providing standards that can adapt to different legal contexts.

The rapid evolution of digital markets requires regulatory frameworks that are both principled and adaptable. The unified framework proposed here represents a contribution to developing constitutional responses adequate to the challenges of concentrated private power in digital markets, preserving the normative authority of constitutional rights while enabling the technical sophistication necessary for effective platform oversight.

Funding
This article received no funding.

Declaration of Conflict of Interests
The authors declared no potential conflicts of interest with respect to the research, authorship and publication of this article.

Declaration about the scope of AI utilization
The authors declared using AI tools in the preparation of this article.