THE PRIVACY-COMPETITION NEXUS: A NEW FRONTIER IN ANTI-TRUST LAW

- Satya Rai & Varsha Agarwal[***]

ABSTRACT

*In an era where every click leaves a digital imprint and consent to privacy policies precedes online interactions, privacy transcends the realms of constitutional courts. Privacy intersects with diverse domains, and one such interface where it is manifesting prominently is in the realm of competition law. This paper explores this intersection by illuminating the evolution of privacy as a cherished consumer value. Then, delving into pivotal moments such as the recognition of privacy as a fundamental right in 2017 and the enactment of the Digital Personal Data Protection Act, 2023 ("**DPDPA/the Act**"), this paper examines its implications for competition regulation, scrutinizing the stance taken by the Competition Commission of India (CCI) on privacy issues. Finally, it concludes by exploring potential avenues for integrating privacy considerations within the existing framework of the Competition Act, of 2002 ("**CA, 2002**").*

[***] The authors are fifth-year students at National Law University, Jodhpur, and can be reached at satya.rai@nlujodhpur.ac.in.

I. INTRODUCTION

The digital age, powered by the Internet of Things (IoT), artificial intelligence (AI), and big data analytics, has transformed how we live and how businesses operate and compete. This transformation has been accompanied by an unprecedented collection and analysis of personal data, turning privacy into a cornerstone issue.

Consumer data has become the lifeblood of the digital economy, driving the business models of tech giants such as Google, Facebook (now Meta), Amazon, and Apple. These companies accumulate vast amounts of data, which they use to personalize advertising, refine services, and, in some cases, entrench their market positions.

For instance, phone users should have the freedom to select apps on their phones, especially considering the data collection practices associated with these apps. However, Google engaged in exclusive agreements with phone manufacturers to pre-install its apps, leading the European Commission in 2018 to deem this practice anticompetitive on account of abuse of dominance. It fined Google €4.34 billion for using Android as a vehicle to cement its market dominance. [1] For the same issue, it faced penalties before the CCI in 2022.[2]

Similarly, the Cambridge Analytica scandal serves as a glaring example of how Facebook user data was used to psychologically sway the voting behaviour of Facebook users in the United States presidential elections. Despite the Federal Trade Commission ("FTC") imposing a $5 billion fine on Facebook, it has been criticised for not looking at the unjust enrichment of Facebook by such a violation. The FTC action has been further scrutinized for its failure to adequately address the privacy infringements and other harms stemming from Facebook's unauthorized exploitation of approximately 87 million user data profiles. [3]

Thus, it becomes increasingly apparent that privacy considerations have permeated the domain of competition law, leading to the growing scrutiny surrounding data practices in digital marketplaces. Now, let us delve deeper into how privacy has evolved into a cherished consumer value.

---

[1] 'Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android Mobile Devices to strengthen dominance of Google's search engine' (European Commission, July 18, 2018) <https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581>.

[2] Indian Express, 'Google fined by CCI for anti-competitive practices on Android: A look at what it says' (October 21, 2022), <https://indianexpress.com/article/technology/tech-news-technology/google-fined-by-cci-1337-crore-android-device-order-key-points-what-it-says-8222776/>.

[3] Margaret Hu, 'Cambridge Analytica's black box' (2020) 7(2) Big Data & Society <https://journals.sagepub.com/doi/full/10.1177/2053951720938091>.

II. PRIVACY AS A CONSUMER VALUE

"*Every successful competitive practice has victims. The more successful a new method of making and distributing a product, the more victims, the deeper the victims' injury.*"

– Judge Frank Easterbrook, "The Limits of Antitrust"

Indeed, competition law does not exist in a vacuum; it is intricately intertwined with economics, necessitating a holistic analysis that encompasses both legalities and economic considerations. In this context, it becomes imperative to examine whether privacy has become a cornerstone of consumer values within the marketplace.

A. Privacy as Feature on Which Companies Fight

Customers increasingly want to buy from organizations which they can trust with their data. Cisco releases every year its reports titled "Data Privacy Benchmark Study ('DPBS')" to explore privacy investment and its economic benefits to organizations. According to the 2024 DPBS report, an overwhelming 94% of organizations acknowledge that their customers would not transact with them if they failed to adequately protect customer data.[4] Apart from Cisco, there are similar reports on privacy investment being an opportunity for brands by McKinsey & Company,[5] Forbes,[6] and even Harvard Business Review.[7]

Apple, for instance, has capitalized on this trend by positioning itself as the most privacy-sensitive big technology company. [8] It has a whole page dedicated to informing customers on how their "apps mind their business. Not yours." and the page starts with the line "privacy. That's Apple."[9] One can simply remind themselves of how in 2016, Apple refused to build a backdoor to an iPhone requested by the Federal Bureau of Investigation (FBI) to collect evidence relating to the deadly act of terrorism in San Bernardino.[10] Apple releases several advertisements[11] with taglines

---

[4] 'Privacy as an enabler of Consumer Trust' (CISCO, 2024), <https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2024.pdf>.

[5] Venky Anant, Lisa Donchak, James Kaplan, and Henning Soller 'The Consumer-Data Opportunity And The Privacy Imperative' McKinsey & Company, <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative>.

[6] Stephen Cavey 'Data Privacy: Your Greatest Competitive Advantage' (Forbes, November 1, 2021) <https://www.forbes.com/sites/forbestechcouncil/2021/11/01/data-privacy-your-greatest-competitive-advantage/?sh=5c0a21ca3f7e>.

[7] David Hoffman 'Privacy Is a Business Opportunity' Harvard Business Review, (April 18, 2014), <https://hbr.org/2014/04/privacy-is-a-business-opportunity/>.

[8] Kif Leswing 'Apple is turning privacy into a business advantage, not just a marketing slogan, (CNBC, June 7, 2021) <https://www.cnbc.com/2021/06/07/apple-is-turning-privacy-into-a-business-advantage.html>.

[9] Privacy, Apple, <https://www.apple.com/privacy/> accessed 7 March 2024.

[10] Tim Cook 'A Message to Our Customers' (Apple, February 16, 2016) <https://www.apple.com/customer-letter/>.

[11] Apple 'Privacy on iPhone | Waiting room' (May 24, 2023), <https://www.youtube.com/watch?v=4-7jSoINyq4>.

such as "Privacy, that's iPhone," "*If privacy matters in your life, it should matter to the phone your life is on*" and others.

Similarly, founded in 2008, DuckDuckGo**,** a search engine, has built its brand around privacy, offering users a tracking-free browsing experience as a direct challenge to Google's dominance with its tagline "None of our business."[12]

B. Privacy Looked at While Deciding Substitutes

Cisco from 2019 has also been releasing annual reports titled "Consumer Privacy Survey ('CPS')."[13] It highlights the rising prevalence of "Privacy Actives," – individuals who prioritize privacy and are willing to take action on it, including shifting companies over their privacy policies. The percentage of "Privacy Actives" has been rising year on year with 33% of consumers surveyed turning out to be "Privacy Actives" in the latest report.[14] The survey[15] report found that young consumers, in particular, are increasingly willing to switch with 42% of consumers aged 18-34 identified as "Privacy Actives." Additionally, there is a growing awareness about privacy laws, with 46% of respondents aware of their country's privacy regulations, especially in countries like India (67%).

To illustrate how privacy considerations are increasingly shaping consumer preferences, one can simply look at the "WhatsApp v. others fiasco" that happened after WhatsApp updated its privacy policy in 2021.[16] People were debating whether to join Telegram, Signal, Discord and others to protect their privacy.[17] This fight is still going on, with WhatsApp making snarky remarks on Telegram's privacy.[18] Therefore, it is evident that consumers now look at privacy while choosing alternatives to a product.

---

[12] DuckDuckGo, DuckDuckGo: None of Our Business, (September 21, 2021), <https://www.youtube.com/watch?v=1W706zdVwc0.>.

[13] Cisco 'Generation Privacy: Young Consumers Leading the Way' (2023), <https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2023.pdf?CCID=cc000160&DTID=odicdc000016&OID=otrsc031725>.

[14] *Id.*

[15] *Id.*

[16] Zak Doffman, 'Why You Should Quit WhatsApp As Critical New Update Confirmed' (Forbes, March 6, 2021), <https://www.forbes.com/sites/zakdoffman/2021/03/06/stop-using-whatsapp-after-facebook-apple-imessage-signal-and-telegram-privacy-backlash/?sh=7228aec333e8>.

[17] Kate O'Flaherty 'Is it time to leave WhatsApp – and is Signal the answer?' (The Guardian, January 24, 2021), <https://www.theguardian.com/technology/2021/jan/24/is-it-time-to-leave-whatsapp-and-is-signal-the-answer>.

[18] Times of India, 'WhatsApp has a 'security warning' for Telegram users' (February 15, 2023), <https://timesofindia.indiatimes.com/gadgets-news/whatsapp-has-a-security-warning-for-telegram-users/articleshow/97954912.cms>.

III. THROWING LIGHT ON THE INDIAN PRIVACY FRAMEWORK

"We can freely celebrate the surge of innovation, the rise of AI, the unprecedented speed of technological advancement and the generational breakthroughs in medicine, science and industry, but if we neglect to address the complex questions of IP, Data Privacy & Protection, we would have conquered the sea, yet leave a giant monster lurking at the bottom."

– Peter-Cole C. Onele

In 2017, India recognized the right to privacy as part of Right to Life under Article 21[19] through *K.S. Puttaswamy v. Union of India.*[20] This momentous decision established privacy as a multi-dimensional right, anchored in dignity and autonomy and set forth a rigorous standard for its infringement, including legitimate state aim, suitable means, proportionality, and a balance where benefits must outweigh the harms to privacy. It also has both positive and negative connotations, where on one hand, it places a negative obligation on the state to not infringe on the privacy of individuals and the other puts a positive obligation on the state to enact legislation safeguarding individuals' privacy. Following the Supreme Court's directive to fortify privacy through legislation, the legislature brought the DPDPA,[21] which is still unenforced.

Notably, despite being drafted in 2023, amidst a pervasive use of algorithms and data collection, the Act fails to address it specifically and explicitly. It defines data as "*personal data in digital form*"[22] but it excludes data which is publicly available. This provision effectively enables companies to collect any publicly available data about people from their social media handles, LinkedIn accounts, etc. and there are several examples of this being done.[23] A case in the US, hiQ and LinkedIn[24] exemplifies this loophole. hiQ utilized publicly available LinkedIn member profiles to inform employers of potential flight risks facilitating actions – to ensure better conditions or demote such persons. But either way, the consent of such persons is not taken. LinkedIn sent a cease-and-desist notice to hiQ for this but hiQ refused to comply. Subsequently, in 2022, the Ninth Circuit Court ruled in favour of hiQ and injuncted LinkedIn from obstructing hiQ's access to publicly available LinkedIn member profiles. The court found that LinkedIn also intended to engage in similar

[19] India Constitution, art. 21.
[20] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[21] The Digital Personal Data Protection Act, 2023. [*hereinafter*, *'*DPDPA, 2023*'*].
[22] *Id* at s 2.
[23] Vidya S., 'Beware! A Social Media Post could cost you for your future job' (Business Today, April 03, 2022), <https://www.businesstoday.in/magazine/cover-story/story/beware-a-social-media-post-could-cost-you-your-future-job-327882-2022-03-30>.
[24] *HiQ Labs Inc. v. LinkedIn Corporation*, Case No. 17-16783 (9th Cir. 2022) <https://law.justia.com/cases/federal/appellate-courts/ca9/17-16783/17-16783-2022-04-18.html>.

business, therefore, selectively banning potential competitors from accessing and using data that is publicly available was an act of unfair competition.

Section 4[25] of the act states that the data of a data principal can be only processed either with the consent or for legitimate use and section 6[26] requires consent to be "*free, specific, informed, unconditional and unambiguous with a clear affirmative action, signifying an agreement to the processing of her data for the specified purpose and be limited to such personal data as is necessary for such specified purpose*." Yet, the reality of clicking a simple checkbox to indicate consent, often without a comprehensive understanding of the privacy policy or the algorithmic black box processing the data, dilutes the essence of informed consent. If one looks at how Google search works, google writes that "*to give you the most useful information, Search algorithms look at many factors and signals*,"[27] the vagueness in this terminology is evident. None would know how it exactly works.[28]

Additionally, while Section 8[29] establishes general obligations for data fiduciaries, such as ensuring data security and offering grievance redressal mechanisms, these requirements lack specificity and do not provide clear guidelines for compliance. The vagueness of these provisions leaves much to interpretation. Without clear compliance guidelines, the framework struggles to operationalize privacy protection effectively. Further, the Act permits the cross-border transfer of data[30] with the requirement that the law of the country outside India where the data is processed must provide equal or higher protection for personal data than that in India. However, the absence of specific provisions outlining the required level of protection or concrete steps to be included in the privacy policy enables companies to transfer data within their corporate groups with ease.

In the event of a breach, the data fiduciary is only required to inform the Data Principal and the Data Protection Board,[31] which is deemed sufficient to discharge their duty. Moreover, the maximum penalty under this Act is ₹250 crores,[32] which is fixed and does not vary based on turnover or profits.

---

[25] DPDPA, 2023, s 4.
[26] DPDPA, 2023, s 7(1)(i).
[27] Google, 'How results are automatically generated' <https://www.google.com/intl/en_in/search/howsearchworks/how-search-works/ranking-results/>accessed March 8, 2024.
[28] Jayson DeMers 'How Much Do We Really Know About Google's Ranking Algorithm', (Medium, May 29, 2020), <https://medium.com/swlh/how-much-do-we-really-know-about-googles-ranking-algorithm-ef031586681b>.
[29] DPDPA, 2023, s 8.
[30] Bhavna Sharma & Dhawal Gupta, 'Data Protection Standards for Cross Border Data Transfers in India' (Live Law, May 25, 2023), <https://www.livelaw.in/articles/cross-border-data-transfer-regulations-global-trade-digital-services-data-protection-229472>.
[31] DPDPA, 2023, s 25.
[32] DPDPA, 2023, Schedule.

Therefore, it is evident that neither the DPDPA offer robust protection for citizens' privacy, nor does it address competition issues directly. Now, it is imperative to see how the CCI has tried to work on the interface between privacy and competition law – whether it has been unconcerned or has proactively taken cognizance of the matter.

IV. CCI'S STANCE ON PRIVACY AND COMPETITION REGULATION

"*Privacy is not just a legal obligation; it's a cornerstone of consumer welfare and integrity in the marketplace.*"

In recent years, CCI has been grappling with the intersection of data privacy and competition law, particularly in the context of digital platforms. The *suo motu cognizance* of the WhatsApp privacy policy update in 2021[33] serves as a prime example of how the CCI has approached this issue, but the Commission's stance on privacy extends beyond this single case.

A. The WhatsApp Case[34]

On January 4, 2021, WhatsApp notified its users about an update to its privacy policy. This update required users to consent to sharing their interaction data with business accounts on WhatsApp with Facebook for marketing and advertising purposes. Failure to agree to these terms would result in users losing access to WhatsApp's services. Interestingly, users in the European region were exempted from this data-sharing arrangement due to negotiations with European data protection regulators. This discrepancy highlighted the absence of robust data protection legislation in India.

In response to the public outcry over the privacy policy update, the CCI initiated a suo moto investigation under Section 26(1) of the Competition Act.[35] The Commission observed that the issue extended beyond the domain of data protection law, as the extensive collection and utilization of data could confer a competitive advantage to dominant firms, potentially enabling them to engage in exploitative and exclusionary practices. Thus, the CCI asserted its authority to scrutinize the matter under the lens of competition law.

The CCI's investigation focused on whether WhatsApp's conduct amounted to an abuse of dominance under Section 4 of the Competition Act.[36] The Commission had previously established WhatsApp's dominant position in the relevant market in the Harshita Chawla case.[37] The CCI stated that "in a data-driven ecosystem, the competition law needs to examine whether the excessive data collection and the extent to which such collected data is subsequently put to use or

[33] Updated Terms of Service and Privacy Policy for WhatsApp Users, In re, 2021 SCC OnLine CCI 19.
[34] *Id.*
[35] The Competition Act, 2002, s 26(1).
[36] The Competition Act, 2002, s 4.
[37] Harshita Chawla v. WhatsApp Inc. and others., Case No. 15 of 2020.

otherwise shared have anti-competitive implications, which require anti-trust scrutiny."[38] CCI then went on to note that the 'take it or leave it policy' contained certain ambiguous and vague terms and it could mean the scope of sharing may extend beyond the information categories that have been expressly mentioned in the policy.[39]

However, the CCI did not consider that the existing regulations lack the framework to address the complex situation, given how the element of privacy makes the market different from our understanding of traditional markets.

The WhatsApp case is just one instance of the CCI's recognition of the interplay between data privacy and competition law. The Commission has, on several occasions, expressed its views on the importance of privacy in the context of competition analysis.

It is necessary to keep in mind that the Big Tech Giants have created a huge market for their services which are "free" but the price is paid in terms of data of the users. However, the mere possession of large amounts of data is never a cause for concern.[40] And, in most cases, neither is using this data to produce a better product.[41] But the use of this data to affect competition and not let new entrants enter the market harms the consumers as well as the competition and that's when this use of data becomes problematic. CCI needs to be vigilant about how Big Firms are using the data of the consumers and needs effective mechanisms to deal with the same.

B. Role of Data in Mergers

The CCI has recognized the potential impact of mergers on data privacy and has incorporated this consideration into its merger review process. In cases where merging entities possess substantial amounts of user data, the Commission carefully examines the implications of the consolidated data power on competition and consumer welfare.[42] The CCI assesses whether the merger would grant the combined entity an undue advantage in terms of data accumulation, which could potentially be used to engage in anti-competitive practices or infringe upon users' privacy rights.

[38] *Supra* note 36.
[39] *Supra* note 36.
[40] Joe Kennedy, 'Should Antitrust Regulators Stop Companies from Collecting So Much Data?' (Harvard Business Review, April 17, 2017), <https://hbr.org/2017/04/should-antitrust-regulators-stop-companies-from-collecting-so-much-data>.
[41] *Id.*
[42]The Competition (Amendment) Act 2023, s 6. [*hereinafter*, "the Deal Value Threshold"].

In 2020, the CCI gave a green light to Facebook's (now Meta) acquisition of a 9.99% stake in Jio Platforms.[43] During the review process, the CCI examined the potential impact of the transaction on competition and data privacy.

The CCI noted that both Jio Platforms and Facebook have access to a large amount of data, and the combination of their datasets could potentially lead to a significant concentration of data. The Commission acknowledged that such data concentration might raise concerns about the use of data for anti-competitive purposes or in a manner that violates users' privacy rights**.** CCI noted that though the parties may have incentives to engage in mutually beneficial data sharing in the future, any anti-competitive behaviour stemming from such arrangements could be taken up by the CCI under Sec. 3 and/or 4 of the CA, 2002 in the future.[44]

C. Market Power and Data Accumulation

The CCI recognizes that firms with dominant positions often have access to large datasets, which can be used to entrench their market power and create entry barriers for new players.[45] The possession of extensive user data can provide incumbent firms with a significant competitive advantage, as they can leverage this data to improve their products, target advertising more effectively, and gain insights into consumer preferences.[46]

The Commission has noted that such firms may engage in practices such as exclusive dealing, tying, or predatory pricing, which can harm competition and limit consumer choice.[47] Thus, data serves as a major factor for bigger firms in maintaining their dominant position.

D. Privacy as a Non-Price Factor

The Commission has also acknowledged that the level of privacy offered by a service can be a key differentiating factor and can impact consumer decision-making.[48] The CCI has also stated that

[43] *Combination Registration No. C-2020/06/747* [2020] Competition Commission of India, (June 24, 2020), <http://164.100.58.95/sites/default/files/Notice_order_document/order-747.pdf>.
[44] AZB & Partners, 'CCI Approves Acquisition of Approximately 9.99% of Jio Platforms by Facebook' (November 13, 2020), <https://www.azbpartners.com/bank/cci-approves-acquisition-of-approximately-9-99-of-jio-platforms-by-facebook/>.
[45] *In re: Federation of Hotel & Restaurant Associations of India (FHRAI) and Others* [2020] Competition Commission of India 14/2019, 01/2020 <https://www.cci.gov.in/images/antitrustorder/en/odrer1666182873.pdf>.
[46] Ankit Srivastava and Divyansha Kumar, 'Digital Economy, Data and Dominance: A perspective' 2 Competition Commission of India Journal on Competition Law and Policy 97, 97-120 (2022), <https://ccijournal.in/index.php/ccijoclp/article/view/43>.
[47] *Supra* note 48.
[48] *Supra* note 36.

the degradation of privacy standards by dominant firms could be considered a form of quality degradation,[49] which can have anti-competitive effects.

E. Intersection with Data Protection Laws

The CCI has recognized the need for collaboration and coordination with data protection authorities to address the complex issues arising from the intersection of competition law and data privacy.[50] While the CCI has asserted its jurisdiction over privacy-related matters that have a bearing on competition, the complementary role of data protection regulations in safeguarding consumer interests cannot be denied.

V. INSIGHTS ON PRIVACY, NETWORK EFFECTS, AND COMPETITION LAW

"*Ultimately, arguing that you do not care about privacy rights because you have nothing to hide is no different than saying you do not care about free speech because you have nothing to say*."

– Edward Snowden

A. Issue of Informational Asymmetry

Information asymmetry is a situation of market failure as owing to the imbalance of power the transactions turn out to be inefficient. It can be easily understood through an illustration, consider a medicine that cures cancer. Consumers lack detailed knowledge about the composition and efficacy of a drug, relying on pharmaceutical companies' assertion of its potential to cure cancer, they consume it. However, even after its consumption, it is still uncertain if it has cured cancer because there are so many other things going on.[51]

Information asymmetry is much more common in data-driven marketplaces because asymmetry is not limited merely to the consumers' lack of understanding about how their data is utilized in specific transactions. It extends further, encompassing uncertainties about how companies store, modify, and potentially intertwine individual data with other datasets. Moreover, the prevalent practice of default settings that favour extensive data collection exacerbates this imbalance. Such

[49] *Supra* note 36.
[50] Competition Commission of India, 'Market Study on the Telecom Sector in India: Key Findings and Observations' (22 January, 2021) <https://www.cci.gov.in/sites/default/files/whats_newdocument/Market-Study-on-the-Telecom-Sector-In-India.pdf>.
[51] Federal Trade Commission, 'Competition and Consumer Protection in the 21st Century' (November 06, 2018), <https://www.ftc.gov/system/files/documents/public_events/1418633/ftc_hearings_session_6_transcript_day_1_11-6-18_0.pdf>.

defaults often lead consumers to unwittingly permit the collection, which allows companies to use it to their advantage.[52]

B. Complementary Network Effects

Complementary network effects arise when distinct businesses benefit reciprocally from the growth of one another.[53] In the case of MMT-Ibibio & Oyo case,[54] Oyo (prominent hotel chain) and MMT (leading online travel agency) through strategic agreements capitalized on their respective market dominances to cross-promote services, thereby amplifying their customer reach.

During a Federal Trade Commission (FTC) session on privacy, Big Data, and competition in 2018, the discourse ventured into how mergers might influence a company's motivation to safeguard consumer data. The discussion unveiled two contrasting perspectives:

- Mergers could yield data protection economies of scale, potentially enhancing a larger entity's capability to secure data more effectively than its smaller counterparts.
- Conversely, the reduction of competition post-merger might diminish the incentive to vie on non-price aspects, such as data privacy.[55]

Similarly, when WhatsApp was acquired by Facebook, it assured the regulators that there would be no sharing of data but there have been numerous instances of its violation since 2016[56] to 2023.[57] Such violations happen as there will be mutual benefits to the two if they share the data. This pattern suggests that the potential mutual benefits of data sharing outweigh the commitments made to regulatory authorities. Moreover, the imposition of fines appears to be an inadequate deterrent, as evidenced by Meta's threats to cease operations in Europe in response to stringent data-sharing regulations.[58]

In India, CCI while approving Facebook's acquisition of a 9.99% stake in Jio Platforms recognized the complementary nature of the user data held by both entities, acknowledging the potential for

---

[52] *Id.*
[53] 'What is the Network Effect', (Wharton Online, January 17, 2023), <https://online.wharton.upenn.edu/blog/what-is-the-network-effect/>.
[54] *Supra* note 36.
[55] 'Competition And Consumer Protection in the 21st Century', (Federal Trade Commission, November 07, 2018), <https://www.ftc.gov/system/files/documents/public_events/1418633/ftc_hearings_session_6_transcript_day_2_11-7-18_1.pdf>.
[56] Mohd Irshad, 'WhatsApp's Privacy U-Turn – It's Been Sharing Data with FB for Yrs', (the Quint, January 18, 2021), <https://www.thequint.com/cyber/policy/whatsapp-facebook-data-sharing-has-been-on-since-2016-amid-privacy-u-turns>.
[57] Adam Satariano, 'Meta Fined $1.3 Billion for Violating E.U. Data Privacy Rule' (New York Times, May 22, 2023), <https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html>.
[58] Sam Shead, 'Meta says it may shut down Facebook and Instagram in Europe over data-sharing dispute' (CNBC, February 07, 2022), <https://www.cnbc.com/2022/02/07/meta-threatens-to-shut-down-facebook-and-instagram-in-europe.html>.

synergies between telecommunications and OTT content/application users.[59] CCI still approved the acquisition stating that they are assured that limited data is shared and if, any anti-competitive conduct stems from such data sharing, CCI can take it up later. But in Facebook's operations in the European Union, such assurances are hardly kept.

C. Incorporating In Consumer Welfare Standard

"*Competition is good for consumers for the simple reason that it compels producers to offer better deals – lower prices, better quality, new products, and more choice.*"

– Sir John Vickers, former Chairman of the Office of Fair Trading, U.K.

Historically, the notion of consumer welfare under competition law has been synonymous with ensuring a wide variety of goods at competitive prices. However, as evidenced by the preceding discussion and examples, privacy, alongside product quality, is emerging as a pivotal non-price factor within the realm of consumer welfare standards. It also stands as an integral component of substitutability, forming a cornerstone of the "*countervailing buying power*"[60] wielded by consumers. Furthermore, this evolution is exemplified by the transition from the small but significant non-transitory increase in price ("SSNIP") to a small but significant non-transitory decrease of quality ("SSNDQ") test to define the relevant market in zero-price markets.[61] CCI should also use these new tools and factors, considering that the factors under sections 19(4)[62] and 19(7)[63] are indicative.

D. Harm over Consent is what is looked at by Competition Laws

Section 4 of the DPDPA[64] allows processing of data if the data principal has provided consent or for legitimate purposes, so it is clear that like most data protection regimes, the Indian Data Protection legislation is based on consent. However, if we look at the competition law, it is based on the harm theory, competition authorities look at the harm that the market competition or the consumers might face due to anti-competitive conduct such as combination, abuse of dominance and anti-competitive agreements. Further, the idea of minimal data collection has gone away with the existence of automated decision-making using AI algorithms which collect as much data as possible.

---

[59] *Supra* note 46.
[60] The Competition Act, 2002, s 19(4)(i).
[61] Kristina Nordlander and Agnieszka Kolasinska, 'European Commission updates rules for defining digital markets in its revised Market Definition Notice', ALLEN & OVERY, (February 26, 2024), <https://www.allenovery.com/en-gb/global/blogs/tech-talk/european-commission-updates-rules-for-defining-digital-markets-in-revised-market-definition-notice>.
[62] The Competition Act, 2002, s 19(4).
[63] The Competition Act, 2002, s 19(7).
[64] DPDPA, 2023, s 4.

E. Lack of a Proactive role of the CCI

The CCI's lack of proactiveness, comprehensiveness, and coordination has impeded its ability to regulate data-driven markets and protect consumer interests.

The CCI's assessment of the WhatsApp privacy policy modification[65] and Jio-Facebook transaction[66] shows its failure to fully assess data-sharing and data concentration's privacy impacts. Because of its concentration on abuse of power and anti-competitive implications, the CCI has ignored the wider impact of these transactions on user privacy rights. This restricted approach has precluded the Commission from assessing important issues including data gathering, data sharing, and user data misuse.

The CCI's reactive approach to data-driven mergers and acquisitions has shown its unpreparedness for digital economy concerns. The CCI has wasted opportunities to set clear precedents and avert competition and consumer privacy harm by allowing acquisitions without a careful examination of data concentration risks and addressing anti-competitive conduct after the conduct has taken place. The CCI's inability to evaluate such transactions is due to its absence of a privacy-focused competition analysis approach. Market power abuse and user privacy rights deterioration are possible because of this regulatory gap.

Thus, addressing the complexities at the intersection of privacy, network effects, and competition law requires a holistic and proactive approach. With this understanding, let us now explore potential strategies and actionable steps to navigate these challenges and pave the way for a fair and competitive digital marketplace.

VI. EXPLORING POSSIBILITIES AND THE WAY FORWARD

The way forward for the CCI in addressing the intersection of data privacy and competition law in the digital era should focus on the following key aspects:

- India should follow Germany's lead[67] and amend its competition law to explicitly include zero-price markets within the scope of relevant product markets.
- The CCI must establish **c**lear-cut guidelines for appraising mergers and acquisitions involving entities holding substantial user data, with a commitment to stringent enforcement.

[65] *Supra* note 36.
[66] *Supra* note 46.
[67] Act against Restraints of Competition, (Federal Law Gazette I, 2013, 1750, 3245) s 18(2a).

- Encouraging companies to compete on privacy standards and integrating privacy as an essential non-price factor in their competition analysis. This approach would incentivize firms to offer better privacy protections and foster a market environment that values user privacy.
- The CCI should actively participate in international forums and engage with competition authorities from other jurisdictions to exchange best practices, share insights, and develop a coordinated approach to addressing data privacy and competition issues in the global digital market.

VII. CONCLUSION

"*If you're not paying for the product, then you're the product.*"

– The Social Dilemma, Netflix Documentary

In conclusion, the intersection of privacy and competition law presents a complex and evolving landscape that demands careful consideration. As privacy increasingly becomes a cherished consumer value and a key differentiator in the marketplace, competition authorities must adapt their approaches to ensure that data practices do not undermine fair competition and consumer welfare. The CCI's recent efforts to address privacy concerns within the competition framework are commendable, but more comprehensive guidelines and collaboration with data protection authorities are necessary.

Furthermore, the unique challenges posed by data-driven markets, such as information asymmetry and complementary network effects, require innovative solutions and a re-evaluation of traditional competition analysis tools. As we move forward, striking the right balance between fostering innovation, protecting consumer privacy, and maintaining healthy competition will be crucial.