THE CHALLENGE OF MARKET POWER IN THE BIG DATA ECONOMY: A CRITICAL LOOK AT COMPETITION LAW

Prissha Chawla, B.B.A LL.B. (Hons.), School of Law, UPES

ABSTRACT

The digital age has ushered in a new era of competition, one that transcends national borders. Developed nations with a stranglehold on "big data," the new global currency, are leveraging this resource to gain an unfair advantage in developing countries' domestic markets. This article delves into the legal implications of this phenomenon. We'll begin by examining the complex interplay between big data and competition law. We'll then analyze real-world case studies where big data was used to stifle competition. The article will then explore the urgency of addressing this issue on a global scale. We'll look at existing and proposed legal frameworks like the General Data Protection Regulation (GDPR), the Digital Personal Data Protection Bill (DPDP), and the Digital Market Act (DMA) to see if they offer solutions.

Ultimately, the paper aims to answer two key questions: Is the abuse of big data a genuine threat to fair competition? If so, how can we address it through legislative and policy changes?

By exploring these questions, we can move towards a more equitable global marketplace.

Keywords: General Data Protection Regulations, Global Competition, Neo-colonialism, Indian Laws, Data Privacy.

Introduction

The Dark Side of Big Data: How Powerful Companies Can Squeeze Consumers and Stifle Competition?

The internet has completely changed how businesses operate. In today's digital world, information about consumers, often called "data," is the most valuable asset a company can have. This data helps businesses understand what people want and need, allowing them to create new products and target advertising more effectively. Companies can create better products and services, and we get exposed to things we might actually be interested in.

However, there's a flip side to this data coin.

Most consumers don't realize how much of their data is collected and used. This can lead to problems:

- Privacy Concerns: We don't always know how our data is being used, and it can feel like big companies are constantly watching us.
- Unfair Advantage: Companies like Amazon, Google, and Facebook have become incredibly powerful because they have so much data. This gives them a big advantage over smaller businesses who can't compete.
- Limited Choices: Companies can use data to manipulate what we see online, limiting our options and making it harder for new businesses to get noticed.

This isn't something new, but the laws haven't quite caught up yet. There are loopholes that allow big companies to exploit data privacy laws and gain even more control. This is like a new form of colonization, where a few powerful companies control the market and limit choices for everyone else. This article will explore this grey area where data privacy and competition laws meet. We'll look at real-world examples of how big companies have used data to their advantage and how the law is struggling to keep up. Ultimately, we want to understand the threats this poses to a fair and healthy marketplace where everyone has a chance to succeed.

Big Data: Stifling Competition and Consumer Choice

In today's digital world, data is king. Understanding what people want and buy (including private information) is crucial for any business to succeed. From corner stores to giants like Amazon, everyone collects data. Here's the problem: some companies turn data collection into a business model, exploiting it for massive profits.[1] They gather, analyze, and store your data, then potentially share it with subsidiaries or even other companies for targeted advertising.[2] This happened recently with Meta (formerly Facebook), which was fined a whopping $1.3 billion by the EU for privacy violations related to advertising.[3]

This raises a red flag for competition. By analyzing your data, these "data giants" (Google, Microsoft, Netflix, etc.) can predict your future choices. This not only undermines your "right to be forgotten"[4] (having your data erased), but also creates an unfair marketplace. Imagine a small business trying to compete with a giant who already knows exactly what products or services you'll be interested in. This data misuse essentially creates a "neo-colonialist" market dominated by big data companies, limiting consumer choice and stifling competition.

Big Data: Turning "Right to be Forgotten" into a "Duty to be Known"

The vast collection of big data raises troubling ethical concerns. By capturing every detail about us, it essentially "dehumanizes" individuals and creates a permanent record of our preferences within an algorithm. Before we even know what we want, these algorithms might already have predicted our choices! This obsession with data collection has turned the "right to be forgotten" (having your data erased) on its head. Global companies see this right as a mere inconvenience, prioritizing their ability to sell your information for a profit. They've essentially turned the "right to be forgotten" into a "duty to be known" – not just by them, but by the entire commercial world! Targeted advertising can be a double-edged sword. While it can provide a more personalized online experience, it comes at the cost of your privacy. Every targeted ad is a reminder that your data has been compromised. Here's where this "data advantage" becomes a competition problem. Beyond the privacy concerns, the way big data companies exploit

[1] Bridget Bothello 'What is Big Data and Why is it Important?' (Tech Target, 12 December 2022)
[2] European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy.
[3] Adam Satariano 'Meta Fined $1.3 Billion for Violating E.U. Data Privacy Rules' (The New York Times, 22 May 2023)
[4] General Data Protection Regulations [2016] clause 17.

private information creates a near-monopoly. Only products promoted by these giants reach the intended buyers, effectively shutting out smaller competitors.[5] Competition laws exist to prevent this exact scenario – to ensure a fair playing field where monopolies don't stifle innovation and new businesses have a chance to thrive. The upcoming case studies will illustrate this point further. In essence, targeted advertising disguised as "improved customer experience" creates a market monopoly.[6]

Case Studies

This section explores two key claims:

1. Consumer data can be misused.

2. This misuse can harm healthy market competition.

Case 1: The German Facebook Case: A Turning Point The 2019 – This case marked a significant shift in how data privacy intersects with competition law. It was the first time a company's terms of service were deemed anti-competitive. Here's why: Forced Consent[7]: Facebook shared user data with subsidiaries (like Instagram and WhatsApp) and third parties, without explicit user permission. Users were essentially forced to agree to data collection as a condition of using the platform. Judge Peter Meier-Beck highlighted this lack of choice, calling it "exploitative" of Facebook's dominant market position.[8] Unfair Advantage: Facebook's near monopoly gave them unfair leverage. Users had limited options – either accept their terms or leave the platform. This case sparked discussions about how large platforms like Facebook ("gatekeepers") use their power to stifle competition. This case paved the way for regulations like the Digital Markets Act (DMA). The DMA acknowledges the power these "gatekeepers"[9] hold and aims to prevent them from engaging in unfair practices, including data misuse that eliminates healthy competition[10]. The German Facebook case was a wake-up call. It

[5] Karney 'Competition law in India' (Legal services India, 28 March 2020)
[6] Matthew Johnson 'How does Facebook make money' (Investopedia, 2 December 2022)
[7] Silke Heinz , 'bundeskartellamt hits dont like button on facebook' (Kluwer Competition Law Blog, 11 February 2019)
[8] 'Germany's top court rules against Facebook' (DW News, 24 June 2020) https://www.dw.com/en/germanystop-court-rules-against-facebook-on-usersdata/a53919404#:~:text=In%202019%2C%20Germany's%20Federal%20Cartel,is%20a%20final%20court%20decision..
[9] The Digital Markets Act [2022], clause 5.
[10] Digital Markets Act: Rules for digital gatekeepers to ensure open markets enter into force (European Commission, 31 October 2022)

highlighted how dominant platforms can abuse user data and limit competition. This case, along with regulations like DMA and GDPR, are crucial steps towards a fairer digital marketplace.

Case 2: Matrimony.com v. Google: A Case of Big Data Abuse? - The 2018 case of Matrimony.com v. Google is a prime example of how big data dominance can stifle competition. This is because Google collects massive amounts of user search data, which fuels their targeted advertising business. For instance, they quite some time back, faced a hefty fine in the US for misusing location data for advertising purposes. Further, it also controls a large share of the online search advertisement market in India. The allegation was that Google manipulates search results to favor themselves and other large corporations, regardless of relevance to the user's query.[11] The case also highlighted misleading advertising practices. Top search results weren't necessarily the most relevant, but rather those with the highest bids. This essentially deceives consumers and limits their choices. Also, by prioritizing their own services (Maps, News, Flights) in search results, Google steers users away from competitors[12]. This dominance in online advertising gives them an unfair advantage across other services as well. Matrimony.com v. Google resulted in a fine for Google, citing violations of India's Competition Act. The court found them guilty of denying market access as Google's practices essentially shut out competitors from accessing the market fairly. Secondly, its dominance in one area (advertising) allowed them to unfairly influence another (search results).

Case 3: Facebook and Cambridge Analytica - The Cambridge Analytica scandal (2018) is a prime example of data misuse. Millions of Facebook users unknowingly had their data harvested to create psychological profiles for targeted political advertising. This data was used to influence voter preferences in the 2017 US elections. Public outrage erupted, leading to the "#deletefacebook" movement and the downfall of Cambridge Analytica. This case highlights how Facebook, now known as Meta, is not immune to data breaches. Their business model relies heavily on targeted advertising, often involving selling user data to third parties. Meta has faced multiple fines for such practices. Most recently, a South Korean watchdog penalized them for sharing data of millions of users with unauthorized parties. By exploiting vast amounts

[11] Matrimony.Com Limited vs Google Llc & Others (2018), SCC OnLine Mad 30438
[12] Ibid

of user data, Facebook gains an unfair advantage. Smaller competitors simply can't compete with this level of targeted advertising, hindering fair market competition and innovation.

Legislative Protection in India, EU, US

India

The Digital Personal Data Protection Act 2023 is the latest legislative effort in India to enact a comprehensive data privacy law. It is based on the ethos of the Puttaswamy judgement[13] and the recommendations of the Srikrishna Committee Report, which envisions a 'free and fair digital economy'.[14] The rise of big data has created a complex landscape where data privacy and fair competition intersect. While big data offers valuable insights for businesses, its misuse by dominant players can stifle competition and harm consumers. The DPDP Bill, though still under consideration in India, aims to address these concerns. Let's delve into how the DPDP can potentially promote fair competition while tackling big data abuse:

1. Increased Transparency and Control over Data: The DPDP mandates clear and specific descriptions of the data being collected and its intended use. This empowers users to make informed choices about sharing their data, potentially limiting unfair data collection practices by companies. Also, individuals can access and correct their data, preventing companies from building inaccurate profiles that might unfairly influence targeted advertising or search results. Further, the "right to be forgotten" allows individuals to request the deletion of their data, hindering companies from building long-term profiles that could disadvantage them in future transactions.

2. Levelling the Playing Field for Smaller Businesses: The DPDP offers some compliance exemptions for startups, easing their entry into the market and potentially reducing dominance by established data giants. By empowering individuals with control over their data, the DPDP can limit the ability of large companies to leverage vast data sets to create unfair advantages.

3. Enforcement Mechanisms and Penalties: The DPDP proposes a data protection authority responsible for enforcing the regulations and investigating complaints about data misuse. This can deter companies from engaging in practices that stifle competition. It also

[13] KS Puttaswamy v. Union of India, (2017) 10 SCC 1
[14] Joint Parliamentary Committee Report Summary Personal Data Protection Bill [2019].

outlines penalties for non-compliance, including fines and potential imprisonment for serious offenses. This incentivizes companies to play by the rules and avoid practices that distort competition.

However, Challenges Remain:

- Limited Scope: The DPDP primarily focuses on data privacy and may not directly address all anti-competitive practices related to big data. Additional legislation or amendments might be needed.

- Enforcement Efficacy: The effectiveness of the DPDP depends on the robustness of enforcement mechanisms. Stringent enforcement is crucial to ensure compliance and truly level the playing field.

- Data Anonymization and Aggregation: Companies may attempt to circumvent regulations by anonymizing data or using aggregated data sets. Regulatory frameworks need to address these loopholes.

The DPDP is a significant step towards data privacy and potentially fairer competition in the digital age. However, it's important to recognize that it's one piece of a larger puzzle. Complementing the DPDP with amendments to competition laws can specifically address anticompetitive practices related to big data use. In addition to this, enabling users to easily transfer their data between platforms can empower them to switch service providers more readily, fostering competition. As data flows across borders, international cooperation between regulatory bodies is crucial to ensure consistent enforcement and prevent companies from exploiting loopholes in different jurisdictions.

The DPDP represents a positive step, but it's an ongoing process. Continuous monitoring, evaluation, and potential amendments will be necessary to ensure that it effectively tackles big data abuse and fosters a fair and competitive digital marketplace. Additionally, a multi-pronged approach, including stronger competition law The European Union (EU) has taken a strong stance on both data privacy and fair competition in the digital age, particularly regarding the challenges posed by big data. Here's a breakdown of their key regulations:

European Union

The EU Charter of Fundamental Rights (Article 8) guarantees citizens the right to data protection. This means all data processing must be lawful or have user consent. The General Data Protection Regulation (GDPR) is considered the world's most comprehensive data privacy law. It mandates clear communication about data collection and processing, user rights to access, rectification, and erasure (right to be forgotten), and the right to object to data processing. Article 12 requires companies (data fiduciaries) to clearly explain how they process user data. This explanation must be easy to understand and written in plain language. Articles 13 and 14 ensure users are informed when their data is collected, even if it's done indirectly. The GDPR grants individuals the right to request the deletion of their data (Article 14). Article 21 empowers users to object to how their data is being used.

TFEU Article 102 prohibits dominant companies from abusing their market position. This includes practices that distort competition. German Competition Act acknowledges the role of personal data in establishing market power, further emphasizing the importance of fair data practices. Digital Markets Act (DMA) directly addresses the misuse of consumer data to eliminate competition. It targets "gatekeepers" – dominant tech companies – and outlines compliance measures including prohibition on self-preferencing.

The EU recognizes the evolving digital landscape and plans to introduce further regulations in the coming decade ("Europe's Digital Decade"[15]). This comprehensive approach highlights the EU's commitment to both data privacy and fair competition in the big data eras and international cooperation, will be essential to fully address this complex challenge.[16] United States

The US approach to data privacy differs from the EU. The Federal Trade Commission (FTC) handles both data privacy and competition concerns, aiming to prevent deceptive practices and unfair competition that limit consumer choice. However, unlike the EU's comprehensive GDPR, the US lacks a central law specifically focused on digital privacy. This is despite being home to many of the world's biggest tech companies.

[15] Jan Jan Lowijs and Hugo Atzema ‘The DMA, a landmark law for the digital space’ (Deloitte, 28 December 2022)
[16] Europe’s Digital Decacde: digital targets for 2030’ (European Commission)
[18] American Data Privacy and Protection Act, [2000], s 202.

The US has a proposed law called the American Data Privacy and Protection Act (ADPPA)[18] that aims to be the country's first major data privacy legislation. While it has some positive aspects, it also falls short in some key areas.

Strengths: The ADPPA requires companies to be clear about how they collect and use data, and to obtain user consent. The Act includes specific protections for sensitive data categories and youth privacy.

Weaknesses: The ADPPA doesn't address employee data or anonymized data sets. Individuals can sue for violations, but only after a two-year waiting period with several restrictions, including notifying authorities first.

Overall, the ADPPA is a step in the right direction for US data privacy, but it needs stronger enforcement mechanisms and broader scope to be truly effective. It tackles market dominance through the Sherman Act, which prohibits monopolizing, attempting to monopolize, or conspiring to monopolize a market. While the US lacks a federal data privacy law, California has its own: the California Consumer Privacy Act (CCPA).

Overall, the US approach to data privacy is a patchwork of federal antitrust laws and state specific regulations like the CCPA. This creates a less consistent framework compared to the comprehensive GDPR in the EU.

While California's CCPA offers some data privacy protections similar to the GDPR, the US still lacks a comprehensive federal law. This is especially concerning when it comes to competition in the digital market. The case studies throughout this paper highlight the ways companies can exploit loopholes in current regulations. Existing laws related to big data and its impact on competition seem to be inadequate.

Analysis

Big data misuse, as discussed earlier, is a significant hurdle for fair competition. While the EU has taken strong action with comprehensive data privacy and competition laws, many other countries, including India, lack such a robust framework. This creates a situation where developing countries like India are vulnerable to data exploitation by multinational corporations. In light of this, India needs to prioritize strengthening its data privacy and

competition laws. Revising the DPDP Bill to be more comprehensive, similar to the GDPR, could be a crucial step in this direction.

How is the Misuse of Big data Neo-Colonisation?

The case studies throughout this paper demonstrate how big data misuse significantly impacts competition in the global market. Large tech companies, primarily US-based, have amassed vast troves of data, creating a situation some argue resembles "neocolonialism." These companies leverage this data advantage to gain an unfair edge, stifling competition, as evidenced by cases like Google's dominance in online advertising and the issues surrounding Facebook's data practices in various countries. These cases highlight the urgent need for stricter regulations to prevent big data from becoming a weapon for tech giants to exploit developing nations. The DPDP Act, while establishing clear roles and responsibilities between data owners (principals) and data handlers (fiduciaries), doesn't address the relationships between these companies themselves. This creates a loophole. Companies could potentially exploit this gap by collecting and manipulating user data in ways that favor themselves, essentially tilting the market unfairly in their favor. This could stifle competition in the Indian market.

The current model of offshoring Indian user data and then manipulating the domestic market with it raises serious concerns. This practice essentially strong-arms consumers towards foreign products and stifles competition. The lack of regulation allows big data companies to charge Indian businesses for advertising access to their own citizens' data – an unethical practice. The Indian government's proposed Digital Competition Act and Digital India Act aim to address this very issue. In today's data-driven world, information is a powerful weapon. Just as nations compete for resources, they are now also competing for control over big data. India's efforts to regulate data offshoring are crucial to protect its valuable domestic data and ensure a fair and competitive digital marketplace.

How is Regulation of Digital Competition Going to Aid the Developing Nations?

The concept of competition in the digital market is well-established. Landmark cases involving companies like Facebook and Google[17] have set legal precedents around the world. These cases demonstrate that abusing a dominant market position to stifle competition is illegal. India's

[17] Matrimony.Com Limited vs Google Llc & Others (2018), SCC OnLine Mad 30438.

Competition Act also prohibits companies from using their dominance to unfairly eliminate competitors, upholding the principles of healthy competition. Regulation through digital competition and privacy laws can be a powerful tool to combat big data misuse. These laws can help:

- Control Data Manipulation and Export: Regulations can restrict the way big companies manipulate and export user data. Examples include India's penalty against Google and similar actions by South Korea. These cases highlight the growing global recognition of how big tech manipulates data for market dominance.

- Address the Borderless Nature of Digital Markets: Since the digital market transcends physical borders, regulations need to account for this. International cooperation and strong national frameworks will be crucial to effectively address this challenge.

This paper has argued that the offshoring and manipulation of big data by large tech companies can resemble a form of "neocolonialism," unfairly disadvantaging developing nations.[18] Stronger regulations are urgently needed to address this emerging threat. New laws are crucial to combat big data misuse. India's proposed Digital Competition Act and a revised DPDP Bill that incorporates stricter data transfer controls are positive steps. Revamping data privacy laws should be a priority. A more comprehensive DPDP Bill, inspired by the GDPR, can empower Indian citizens and protect their data. While competition laws play a role, a broader approach is needed. India's focus should be on maximizing domestic market efficiency and fostering fair competition for both consumers and businesses, without hindering global trade.

By enacting robust data privacy laws and fostering international cooperation, India can safeguard its valuable data resources and ensure a fair and competitive digital marketplace for all participants. This will require a multi-pronged approach that goes beyond simply adapting existing competition laws.

Conclusion: Big Data, Neocolonialism, and the Need for a Comprehensive Framework

This article began with a provocative claim: big data can be a tool for neocolonialism. By examining real-world case studies and global legislation around data privacy and regulation, the argument has been substantiated. The vast amount of personal data collected by large

[18] Micheal Kwet, 'Digital Colonialism: The Evolution of the US Empire' (TNI, 4 March 2020)

corporations can be used to gain undue dominance in developing countries' markets. Current data privacy laws, like India's proposed DPDP Bill, while positive steps, may not be comprehensive enough. The DPDP, for instance, lacks the GDPR's strictness on data transfer. To effectively address this "digital neocolonialism," a multifaceted approach is needed:

1. Strengthening the DPDP Bill: The DPDP Bill should be revised to include stricter regulations on cross-border data transfers, aligning it more closely with the initial goals of the Srikrishna Committee report.

2. Digital Competition Act: The proposed Digital Competition Act, with its new committee, is a positive step. This committee can play a crucial role in safeguarding Indian data from exploitation by big tech companies.

3. Data Privacy and Competition Act Alignment: The current data privacy and competition laws in India need to work in greater harmony. This will ensure a more cohesive legal framework that tackles both data privacy concerns and anticompetitive practices.

The Indian government needs to consider these suggestions and potentially overhaul existing data privacy and competition laws. This will be vital to protect India's digital market from the dangers of "digital neocolonialism" driven by big data dominance. The issue of big data and its potential for abuse is constantly evolving. Continuous monitoring and adaptation of legal frameworks will be necessary to stay ahead of emerging threats and ensure a fair and competitive digital landscape for all. International cooperation between regulatory bodies will also be crucial in this endeavor. By combining strong national regulations with international collaboration, we can create a digital world that fosters innovation, protects personal data, and prevents the exploitation of developing nations.