Volume 32, May 2024 ISSN 2581-5504

"Analysing the Digital Dilemma: AI, Competition Law, and Data Privacy in the Age of Tech Giants"

***Shruti Khatri**
Symbiosis Law School,
Nagpur
(Affiliated to Symbiosis International University)

****Shobhna Nayak**
Symbiosis Law School,
Nagpur
(Affiliated to Symbiosis International University)

Introduction

In the rapidly evolving digital landscape, tech giants play a crucial role in advancing Artificial Intelligence (AI) technologies. This research focuses on analysing how companies such as Amazon, Google, Tesla etc., are utilizing AI to transform industries, improve customer interactions and drive innovation[1]. Additionally, it examines the ethical implications and challenges that arise from the integration of AI by these tech giants.

The collection and utilisation of personal data by these tech giants for the AI application raise concerns regarding privacy and data security. Furthermore, it is imperative that Al is utilized solely for ethical purposes, especially in processes such as loan approvals or hiring, where ethical considerations hold paramount importance. As AI continues to reshape industries and create new opportunities, discussions on ethical implications of AI are crucial to ensure responsible development[2]. Tech giants are at the forefront of driving innovation while addressing global challenges through AI technologies.

Major technology companies hold substantial power in influencing the direction of Al development and its application in the digital era. By prioritizing ethical considerations, promoting innovation, and advocating for responsible Al practices, these companies are playing a pivotal role in shaping a future where technology not only enriches human experiences but also mitigates potential risks associated with Al implementation[3]. Essentially, it emphasizes the responsibility of tech giants in steering Al towards a positive and beneficial path for society.

[1] McKinsey. (2024, February 21). The economic potential of generative AI: The next productivity frontier. Retrieved from https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier

[2] Forbes Business Council. (2023, May 12). How Businesses Can Ethically Embrace Artificial Intelligence. Retrieved from https://www.forbes.com/sites/forbesbusinesscouncil/2023/05/12/how-businesses-can-ethically-embrace-artificial-intelligence/?sh=4058588520a3

[3] Frontiers in Surgery. (2022, February 18). Legal and Ethical Consideration in Artificial Intelligence in Healthcare. Retrieved from https://www.frontiersin.org/articles/10.3389/fsurg.2022.862322.

Volume 32, May 2024 ISSN 2581-5504

Importance of Competition Law and Data Privacy

The importance of competition law lies in promoting fair market competition, fostering innovation, protecting consumer welfare, preventing monopolistic practices, encouraging efficiency, and ensuring a level playing field for businesses of all sizes. On the other hand, data privacy regulations are crucial for safeguarding personal information, preserving individual rights, preventing abuse by companies, fostering trust and reputation, and facilitating cross-border data flows.

In India, the protection of personal information is addressed through the intersection of competition law and data privacy regulations. The Competition Commission of India (CCI) plays a role in regulating concerns related to privacy within the digital economy. The CCI's understanding of competition law extends to include privacy as a non-price parameter of competition, emphasizing the importance of data privacy in maintaining fair market practices. The Digital Personal Data Protection Act (DPDPA) aims to regulate the processing of digital personal data while balancing individual rights and has raised questions about how the CCI should navigate spaces where privacy law and competition law overlap. The CCI's intervention in matters of privacy, such as in cases like WhatsApp's data-sharing practices with Facebook, demonstrates its authority in addressing privacy concerns that could lead to anti-competitive behavior.

However, to establish a violation of competition law, there must be evidence of misconduct that undermines fair competition. This means that the conduct in question must not only involve mishandling data and infringing on users' privacy but also have a detrimental impact on competition itself. It's important to note that simply reducing privacy protections doesn't automatically translate into a competition issue. Similarly, not every instance of reduced privacy immediately constitutes a breach of data protection law, especially if the data processing practices adhere to legal requirements. In essence, while privacy infringements may be a component of competition law violations, they must be accompanied by actions that distort or harm market competition to warrant regulatory intervention.

Overall, it's important to maintain a clear distinction between competition law and data protection regulations. While privacy considerations are relevant to competition analysis as a qualitative factor, it's essential to preserve the independence of these legal domains. This ensures that each regulatory framework can fulfill its objectives effectively without conflating their purposes. By maintaining this analytical independence, regulatory authorities can enhance predictability and uphold the rule of law, ultimately contributing to a more transparent and lawful business environment. Effective enforcement and coordination between competition law and data privacy regulations are essential for creating an environment where businesses can thrive while respecting individuals' rights and privacy in the digital economy, including within the context of Indian laws.[4]

[4] Interplay between Data Protection and Competition Law, AMLEGALS (Feb. 19 2024), https://amlegals.com/interplay-between-data-protection-and-competition-law/.

Volume 32, May 2024 ISSN 2581-5504

Understanding Artificial Intelligence interplay between Competition and Data Protection

Artificial Intelligence (Al) has emerged as a potent force driving societal change, presenting a multitude of advantages alongside challenges in terms of competition and safeguarding data. In the contemporary landscape, the nexus between Al and law, particularly concerning data protection, has taken centre stage, given the extensive processing of personal data inherent in many Al applications[5]. While Al holds the potential to augment human capabilities, enhance security, and foster efficiency, it also introduces risks such as increased potential for control, manipulation, and discrimination, along with disruptions to social interactions and exposure to harm resulting from technological failures disregard for individual rights and social values[6].

The past decade has witnessed substantial growth in the global digital industry, including within India, leading to the advent of novel business models and operational efficiencies. However, this expansion has prompted concerns regarding the potential manipulation of data by Information Technology (IT) companies[7]. Specifically, mergers driven by data-centric strategies within the tech industry aim to provide personalized services but also pose risks to competition dynamics by compromising data privacy and creating barriers to market entry[8].

Al technologies not only present privacy risks but also offer the potential to improve it. Many companies utilize Al tools to ensure compliance with privacy and cybersecurity regulations[9]. For example, Al-driven methods enable the immediate identification of sensitive data across various environments, followed by the implementation of privacy measures such as tokenization to safeguard the data. Notably, a 2019 study by Gartner projected that by 2023, 40 percent of privacy compliance technology would integrate Al, a forecast likely exceeded by the present time[10]. Moreover, Al can enhance data protection against unauthorized access through mechanisms like intrusion detection systems equipped with Al to detect fraudulent patterns and authentication techniques utilizing Al to deter hackers[11].

Businesses across sectors are harnessing Al to improve operational efficiencies and gain competitive advantages. Notably, Dentons, a key player in the industry, has demonstrated its

---

[5] Panel for the Future of Science and Technology: EPRS | European Parliamentary Research Service, ISBN: 978-92-846-6771-0, Law, State and Telecommunications Review. (2021, September 7). AI Training Datasets & Article 14 GDPR: A Risk Assessment for the Proportionality Exemption of the Obligation to Provide Information.

[6] The 15 Biggest Risks of Artificial Intelligence, https://www.forbes.com/sites/bernardmarr/2023/06/02/the-15-biggest-risks-of-artificial-intelligence/?sh=58deb4852706, Forbes, March 24, 2024

[7] NITI Aayog. (2022). India's Booming Gig and Platform Economy: Perspectives and Recommendations on the Future of Work. June, 2022.

[8] EDUZONE: International Peer Reviewed/Refereed Multidisciplinary Journal (EIPRMJ), ISSN: 2319-5045 Volume 8, Issue 2, July-December, 2019, Impact Factor: 5.679, Available online at: www.eduzonejournal.com

[9] AI and Privacy: The privacy concerns surrounding AI, https://economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy-concerns-surrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cms?from=mdr March 24, 2024

[10] Gartner, https://www.gartner.com/en/newsroom/press-releases/2020-02-25-gartner-says-over-40-percent-of-privacy-compliance-technology-will-rely-on-artificial-intelligence-in-the-next-three-years- 25, March 2024

[11] Ramanpreet Kaur, Artificial intelligence for cybersecurity: Literature review and future research directions, Information Fusion Journal, Volume 97, Year-2023, Issn- 1566-2535, 25 March, 2024.

Volume 32, May 2024 ISSN 2581-5504

commitment to innovation by introducing FleetAl, a state-of-the-art solution tailored to client needs. This strategic initiative not only underscores Dentons' forward-thinking approach but also highlights Al's transformative potential in driving business success[12].

Entities like the Competition Commission of India (CCI) have initiated investigations into major players such as WhatsApp, Facebook, and Google to address concerns regarding data manipulation[13]. However, the application of Competition Law in this context presents questions and challenges[14]. Despite the absence of dedicated Data Protection Law, it is crucial to recognize the Right to Privacy as a fundamental right falling under the state's purview[15].

Incidents like the data breaches at Air India and Domino's in 2021 in India underscore the nation's digital vulnerabilities, emphasizing the need for heightened cybersecurity awareness and preparedness across generations[16].

The CCI characterizes data usage as 'non-price competition' in its Telecom Report, suggesting that organizations leverage consumer data to gain competitive advantages[17]. However, this can lead to abusive behaviors such as poor privacy standards, inadequate data security, and exploitation of data advantages across services[18].

Balancing data-driven technologies for competitive advantage with compliance with legal and ethical standards surrounding data privacy and competition is imperative for businesses. The interplay between Competition Law and Data Protection Law is complex and evolving, with differing viewpoints on how these legal frameworks should interact, namely the Separatist View and the Integrationist View.

In India, it is crucial for the Competition Commission of India (CCI) to collaborate with other entities tasked with formulating Data Protection Norms. Prompt enactment of clear and thorough Data Protection laws is imperative to facilitate efficient regulation, promote innovation, and uphold trust in the digital realm[19].

Poor privacy standards, indicating a disregard for customer welfare. Inadequate data security, potentially indicative of exclusionary practices. Exploitation of data advantages across multiple services.

[12] Managing the competition law risks of AI, https://www.dentons.com/en/insights/articles/2023/november/17/managing-the-competition-law-risks-of-ai March 25, 2024
[13] Report of the Committee on Digital Competition Law, Ministry of Corporate Affairs Government of India, https://www.cci.gov.in/images/antitrustorder/en/142019-and-0120201652511256.pdf March 24, 2024
[14] Ibid
[15] Ibid
[16] The biggest data breaches in India (May 30, 2021), https://www.csoonline.com/article/569325/the-biggest-data-breaches-in-india.html, CSO Online- May 30, 2021
[17] Supra 12
[18] Supra 12
[19] Supra 15

Volume 32, May 2024 ISSN 2581-5504

Companies should utilize Al in a manner that does not contravene data privacy laws or infringe upon competition regulations. It is imperative for businesses to strike a balance between utilizing data-driven technologies for competitive advantage while ensuring compliance with legal and ethical standards surrounding data privacy and competition.

The interplay between Competition Law and Data Protection is a complex and evolving issue that requires careful consideration. Two main viewpoints, the Separatist View and the Integrationist View, offer contrasting perspectives on how these two legal frameworks should interact[20].

The Separatist View contends that Competition Law and Data Protection Law should be kept distinct and not overlap. Proponents of this view argue that incorporating privacy and data protection concerns into Competition Law assessments could lead to confusion, particularly in evaluating standards of consumer welfare[21]. This view is rooted in legal precedent, such as the Asnef-Equifax v Asociación de Usuarios de Servicios Bancarios case, which emphasizes the need to treat Data Protection Law and Competition Law as separate entities[22].

In India, it is imperative for the Competition Commission of India (CCI) to collaborate with other authorized bodies responsible for developing Data Protection Norms. While the CCI can address anti-competitive practices deviating from these norms, attempting to define what constitutes an "excessive amount of data" might lead to conflicting positions with authorities better equipped to make such assessments. Urgent action is required to implement clear and comprehensive Data Protection laws without delay. If such legislation establishes thresholds for data collection, the CCI could then appropriately analyze market power in digital marketplaces, yet precedence should be given to Data Protection Authorities in these matters. To enhance collaboration between the two regulatory bodies, Sections 21 and 21A of the Competition Act should be revisited, as the current provisions lack effectiveness due to non-compulsory and non-binding consultations between the authorities[23].

In the evolving landscape of artificial intelligence (Al), the interplay between competition law and data protection presents a nuanced challenge, with Al technologies offering both opportunities for enhanced efficiency and risks to privacy and fair competition. While Al-driven innovations hold promise in bolstering data protection measures, such as automatic detection of sensitive data and cybersecurity enhancements, they also raise concerns regarding privacy breaches and abusive corporate practices. Collaboration between regulatory bodies, exemplified by the Competition Commission of India (CCI) and other data protection authorities, is crucial to developing coherent frameworks that balance the benefits of Al-driven

[20] Nikhil Sharma and Sachin Kapoor, International Journal of Core Engineering & Management (IJCEM) Volume 2, Issue 8, ETHICS: IT'S RELATION WITH INDIAN SCRIPTURES AND BUSINESS, ISSN- 2348 9510
[21] Competition Law And Privacy: An Opinion on The Future of a Complicated Relationship (June 08, 2022), https://competitionlawblog.kluwercompetitionlaw.com/2022/06/08/competition-law-and-privacy-an-opinion-on-the-future-of-a-complicated-relationship/, Kluwer Competition Law Blog- March 25, 2024
[22] Ibid
[23] Supra 15

Volume 32, May 2024 ISSN 2581-5504

competition with the protection of individual privacy rights. Urgent action is required to establish clear and comprehensive data protection laws, enabling effective regulation while promoting innovation and maintaining trust in the digital sphere.

The Impact of Interoperability on Data Protection and Competition Laws: An Analysis

Interoperability significantly influences competition dynamics and the landscape of data privacy laws by fostering innovation, expanding consumer choices, and protecting user privacy. Firstly, interoperability promotes competition by breaking down barriers to entry and reducing the dominance of incumbent players. When systems and applications can seamlessly communicate and exchange data, new entrants find it easier to introduce innovative products or services, thereby challenging established market players. For instance, in the realm of social media, interoperability could enable users across different platforms to interact seamlessly, mitigating the monopolistic power of dominant players and encouraging a more competitive environment.

Moreover, interoperability stimulates innovation by enabling developers to build upon existing technologies and create novel solutions. When different systems can interoperate effectively, developers can focus on adding unique features and functionalities rather than reinventing basic functionalities. This spurs technological advancements and benefits consumers by offering them more diverse and advanced products and services.

Additionally, interoperability aligns with data privacy laws by ensuring that user privacy is safeguarded throughout data exchange processes. Regulations like the GDPR and CCPA impose stringent requirements on how companies handle and process user data, necessitating robust data protection measures in interoperable systems, such as encryption, user consent mechanisms, and anonymization techniques.

Furthermore, interoperability facilitates data portability, empowering users to transfer their data between different platforms and services seamlessly. This capability reduces lock-in effects and promotes competition by enabling users to switch between providers without losing their data. Data portability also enhances user control over personal information, aligning with principles of data sovereignty and fostering trust in digital ecosystems.

Additionally, interoperability can serve as a regulatory tool to address antitrust concerns. Regulators may mandate interoperability between dominant platforms and smaller competitors to level the playing field and prevent anti-competitive practices. This regulatory approach aims to promote fair competition and prevent monopolistic behavior that may stifle innovation and harm consumers.

In conclusion, interoperability's impact on competition and data privacy laws is multifaceted. It fosters competition by promoting innovation and expanding consumer choices while ensuring that data exchange processes adhere to stringent privacy regulations. Furthermore, interoperability facilitates data portability, enhances user control over personal data, and can be leveraged as a regulatory tool to address antitrust concerns. Achieving a balance between

Volume 32, May 2024 ISSN 2581-5504

interoperability, competition, and data privacy necessitates careful consideration of regulatory frameworks and industry standards to create an environment conducive to innovation while safeguarding user rights and promoting fair competition.

The new upcoming Digital Competition Act can make a significant difference in handling issues like interoperability by mandating provisions that promote data sharing, portability, and interoperability among digital entities. By requiring digital platforms to share their application programming interfaces (APls) and facilitate seamless interoperability, the legislation aims to enhance user choice, promote market contestability, and mitigate the risks of market foreclosure and monopolization. This proactive approach can foster a more competitive digital ecosystem, encourage innovation, and safeguard consumer welfare by ensuring fair access to digital services and promoting a level playing field for all market participants.[24] [25]

Case Studies: Exploring the Antitrust Conundrum with AI and Big Data

EU vs. Amazon and Google's Antitrust Battles:

I. EU vs. Amazon – Amazon's Superpower: Friend or Foe to Sellers?

The Scenario:

- Amazon is a bustling marketplace, where independent sellers can offer their wares alongside Amazon's own products. This dual role raises eyebrows- is Amazon both "landlord" and "competitor"? Concerns arise about unfair competition and Amazon potentially using sellers' data against them.

The EU investigation into Amazon highlights how AI and Big Data raise concerns about anti-competitive practices within online marketplaces:

- Amazon, like many tech giants, collects vast amounts of data on seller activity, consumer behaviour, and product trends. This data can be fed into AI algorithms that personalize search results, recommend products, and decide which products are displayed prominently. The EU was concerned that Amazon might use this data to favor its own products in search results or manipulate algorithms to disadvantage third-party sellers on its marketplace. Essentially, AI facilitates the analysis of this vast data trove, potentially leading to unfair advantages for Amazon.

- The EU also expressed concerns about the potential bias inherent in algorithms used by Amazon. These algorithms are trained on massive datasets, which can perpetuate existing biases or create new ones. For example, an algorithm trained on historical data

[24] Data portability, interoperability and digital platform competition, OECD (2021), https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF%2FCOMP%2FWD%282021%2944&docLanguage=En.

[25] "Interoperability of Digital Platforms May Raise User Security Risks," Business Standard (February 14, 2024), https://www.business-standard.com/technology/tech-news/interoperability- of-digital-platforms-may-raise-user-security-risks-124021400916_1.html.

Volume 32, May 2024 ISSN 2581-5504

showing Amazon products being more frequently purchased might continue to favor those products over equally competitive offerings from third-party sellers. Here, AI itself doesn't create bias, but the data used to train it can lead to biased outcomes.

- The lack of transparency around how Amazon's algorithms work further compounded the EU's concerns. Without knowing the specific criteria used by the algorithms, it's difficult to assess whether they are treating all sellers fairly.

The EU Accusation (2020):

- The European Commission, Europe's competition watchdog, took action.
- They accused Amazon of using non-public data from independent sellers, like product prices and sales volumes, to:
    - Set its own prices and undercut sellers
    - Develop similar, competing products based on seller data
    - Favor its own products in search results

    The European Commission investigated Amazon on two main points:

    - Data Advantage: The EU investigated whether Amazon used data from third-party sellers on its marketplace (like sales figures) to compete unfairly against those same sellers by giving its own products preferential treatment.
    - Market Dominance: The EU examined whether Amazon's role as both a seller and a marketplace operator gave it an unfair advantage, specifically regarding the "Buy Box" (the featured seller spot for a product) and "Prime" program (premium membership with faster delivery).

Issues:

- This practice allegedly stifles competition: if small sellers can't compete with Amazon's data-driven advantage, it discourages choice and innovation.
- It raises concerns about data privacy: are sellers unknowingly giving Amazon a weapon to use against them?

Current Situation:

- The antitrust investigations are closed, with Amazon subject to the agreed upon changes.

Investigations and Outcomes:

- 2019: The EU opened an investigation into Amazon's use of seller data.
- 2020: A second investigation began, looking at how Amazon selects BuyBox winners and Prime program participants.
- 2022: Amazon agreed to address the EU's concerns by:
    - Not using seller data for its own retail business.
    - Ensuring a fair selection process for the Buy Box, giving all sellers a shot.

Volume 32, May 2024 ISSN 2581-5504

- Granting equal access to the Prime program for qualifies sellers.[26] [27]

II. Google vs. EU Antitrust Battles: A Breakdown of Each Case

1. Comparison Shopping Showdown (2017):

This case centered on the accusation that Google abused its dominant search engine market position to unfairly favor its own comparison shopping service, Google Shopping, in search results. Here's a breakdown of the key details:

The Accusation:

- The European Commission (EU) brought an antitrust case against Google, The EU claimed Google displayed Google Shopping results more prominently than those from competing comparison shopping services.
  This practice disadvantaged competitors and limited user choice, even if competitors' services might be objectively more relevant to the user's search query.

Analogy: Imagine searching for "running shoes" and seeing mostly shoe stores owned by Google listed at the top, pushing down results from other stores.

The Defense:

- Google argued their search algorithm prioritized relevance and user experience.
- They claimed Google Shopping results were often genuinely the most relevant to user searches.

The Outcome:

- 2017: The EU fined Google a record-breaking €2.42 billion (US$2.7 billion) for this violation.
- Google was ordered to make changes to its search results page to ensure:
  - Fair competition: All shopping comparison services receive equal treatment.
  - Transparency: Google Shopping results are clearly marked as Google's own product.
  - Auction system (partially implemented): An auction system might be used to determine the order of shopping comparison service results, though Google retains some control over the process.

Current Situation:

- Google has made changes to its search results page as mandated by the EU.
- This case is a landmark ruling promoting fair competition in the search engine market.

[26] Harvard Business Review, "Understanding the Tradeoffs of the Amazon Antitrust Case," January 11, 2024, https://hbr.org/2024/01/understanding-the-tradeoffs-of-the-amazon-antitrust-case.
[27] The New York Times, "Amazon Set to Face Antitrust Charges in European Union," June 11, 2020, https://www.nytimes.com/2020/06/11/technology/amazon-antitrust-european-union.html.

Volume 32, May 2024 ISSN 2581-5504

- However, the debate about search engine bias continues, with some critics arguing that Google may still subtly favor its own products despite the mandated changes.[28] [29] [30]

2. Android's Anti-Competitive Armor (2018):

- This case focused on the EU's claim that Google leveraged its dominance in the Android mobile operating system to stifle competition in search engines and browsers. Here's a breakdown of the key details:

The Accusation:

- The European Commission (EU) charged Google with anti-competitive practices related to the Android mobile operating system. The EU claimed Google forced Android phone makers to pre-install Google apps like Search and Chrome on their devices. This practice disadvantaged competing search engines and browsers by making it more difficult for users to discover and use them.

Analogy: Imagine buying a new phone and it only allows you to use Google Maps to navigate, even if other navigation apps might be better suited for your needs.

The Defense:

- Google argued that pre-installing their apps benefited users by providing a consistent and familiar experience across Android devices.
- They also claimed that since Android is open-source, phone makers were not restricted from installing other apps.

The Outcome:

- 2018: The EU fined Google a hefty €4.34 billion (US$5.04 billion) for this conduct.
- Google was ordered to stop the practice of forcing phone makers to pre-install Google apps.
- The EU also mandated that Google allow phone makers to develop alternative versions of Android without Google's apps pre-installed.

Current Situation:

- Google is appealed that the fine was too high and the restrictions imposed by the EU on how they handle Android were unjustified because the users will always have the option to again install apps according to their own wish, google is not restricting that in anyway.

[28] SSRN, "Google v Commission (Google Shopping): A Case Summary," November 29, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3965639.
[29] European Commission, "CASE AT.39740 Google Search (Shopping) ANTITRUST PROCEDURE," June 27, 2017, https://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf.
[30] Kluwer Competition Law Blog, "Google Shopping: The General Court takes its position," November 15, 2021.

Volume 32, May 2024 ISSN 2581-5504

- The case has significant implications for the way dominant tech companies control operating systems used on mobile devices.
- If the EU wins the appeal, it could force Google to change its practices worldwide, not just in Europe.

3. AdSense's Exclusive Enclave (2019):

- This case centered on the EU's claim that Google restricted how websites could display advertising, limiting competition in the online advertising market. Here's a breakdown:

The Accusation:

- The European Commission (EU) accused Google of anti-competitive practices related to its AdSense advertising service. The EU found that Google restricted third-party websites from placing ads from its competitors on their sites using its AdSense advertising service, limiting advertising options for smaller players. This practice limited advertising options for website owners and potentially stifled competition in the online advertising market.

Analogy: Imagine a company that owns all the billboards in a city and only allows them to show its own advertisements, forcing businesses to use them or miss out on reaching potential customers.

The Defense:

- Google argued that restrictions were necessary to maintain the quality of ads displayed on websites using AdSense.
- They claimed competing ads might be malicious or inappropriate for their platform.

The Outcome:

- 2019: The EU fined Google €1.49 billion (US$1.7 billion) for this anti-competitive behavior.
- While the specific details of the settlement are not publicly available, it's likely Google agreed to modify its practices related to allowing competitor ads on websites using AdSense.

Current Situation:

- There's no mention of an appeal by Google in publicly available information.

Volume 32, May 2024 ISSN 2581-5504

- This case highlights the EU's scrutiny of Google's dominance in the online advertising market. The outcome might have encouraged Google to allow more competition within the AdSense platform.[31] [32]

In the EU vs. Amazon case, concerns were raised about Amazon's dual role as a marketplace operator and seller, potentially giving it an unfair advantage over third-party sellers. This mirrors the accusations against Google in the EU antitrust battles, where the search engine giant was accused of favoring its own products, such as Google Shopping, in search results, disadvantaging competitors.

Both cases highlight the EU's commitment to ensuring fair competition in the digital market by investigating and taking action against tech giants engaging in anti-competitive practices.

Microsoft's Integration Practices and Facebook's Data Practices:

III. Microsoft and Integration Practices: A Tale of Two Eras

Chapter 1: The Browser Wars (1998)

- Microsoft, the PC King: Microsoft dominated the personal computer market with its Windows operating system.
- Netscape Navigator, the Rival: Netscape's web browser threatened Microsoft's control over the Internet experience.
- The Monopoly Accusation: The US government sued Microsoft for abusing its monopoly to crush Netscape. They claimed Microsoft illegally bundled its own browser, Internet Explorer, with Windows to edge out Netscape.
- The Verdict (1998): Microsoft was found guilty of violating antitrust laws and forced to change its practices.[33] [34] [35]

Chapter 2: Microsoft and The LinkedIn Data Debate: A Multi-Angled Analysis

- The Acquisition: Microsoft purchased LinkedIn, the social networking platform for professionals, in 2016.
- Integration Plans: Microsoft announced plans to integrate LinkedIn data into its various products, like Office and Dynamics.

[31] Wikipedia, "Antitrust cases against Google by the European Union," https://en.wikipedia.org/wiki/Antitrust_cases_against_Google_by_the_European_Union.
[32] Reuters, "Google loses challenge against EU antitrust decision, other probes loom," September 14, 2022, https://www.reuters.com/technology/eu-courts-wed-ruling-record-44-bln-google-fine-may-set-precedent-2022-09-14/.
[33] Arbelaez, Camilo, et al. *Machine Learning and Antitrust: A Comprehensive Review.* SSRN, 2022. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3965639.
[34] *Yale Law Journal: Vol. 132.* Yale Law Journal, 2022. https://www.yalelawjournal.org/files/Volume132StyleGuiderev.2022.11.02_nqty59xo.pdf.
[35] Lemley, Mark A., and Shubha Ghosh. *Antitrust Law: Cases and Materials.* Foundation Press, 2019. https://ir.law.utk.edu/cgi/viewcontent.cgi?article=1751&context=utklaw_facpubs.

Volume 32, May 2024 ISSN 2581-5504

- Privacy Concerns: This sparked worries about how Microsoft would use LinkedIn's vast treasure of user data:
    - Would it combine data without user consent?
    - Could it create unfair advantages in advertising or other areas?

Hence, Microsoft's proposed acquisition of LinkedIn in 2016 raised concerns about data privacy, competition, and the potential for market dominance.

The deal garnered scrutiny from various authorities, including:

- US Department of Justice Antitrust Division (DOJ)
- European Commission (EU)
- Federal Trade Commission (FTC)
- Data protection authorities in various countries.

Angles of the Case:

- Data Privacy:
    - Data Pooling: The biggest concern was the vast amount of user data now under one roof. This included professional information on LinkedIn (resumes, skills, job history) and personal data from Microsoft products (emails, documents).
    - Data Sharing: How this combined data pool would be used and shared was a major question. Could Microsoft leverage LinkedIn data for targeted advertising or influence job searches on LinkedIn based on a user's Microsoft activity?
    - Lack of Transparency: There is scope for the users to seek clarity about the level of transparency regarding data collection, usage, and potential sharing practices.

- Potential Harm to Competition:
    - Concerns arose about Microsoft gaining an unfair advantage by leveraging LinkedIn data to dominate against smaller competitors in the online recruitment market.
    - Opponents argued it could stifle competition from smaller job boards and professional networking platforms.
    - Less innovation in the online recruitment and professional networking space due to Microsoft's dominant position.
    - Reduced options and higher prices for employers and job seekers due to a lack of competitive pressure.
    - Cross-Selling Opportunities: Microsoft's ability to cross-sell its products, such as Office 365 and Teams, with its other offerings can be seen as an unfair advantage. This could lead to a situation where competitors are unable to effectively compete with Microsoft's integrated product offerings.
    - Enhanced Data Analytics Capabilities: Microsoft's enhanced data analytics capabilities for talent management and workforce planning can be seen as an unfair advantage, as it may allow the company to make more informed decisions about its

Volume 32, May 2024 ISSN 2581-5504

workforce than its competitors. This could lead to a competitive advantage that is difficult for other companies to replicate.

- Market Dominance:
  - The combined entity's potential dominance in the professional networking and online recruitment spaces was a major concern.
  - Critics feared it could lead to higher prices, reduced choice, and stifling of innovation.

Microsoft's integration with LinkedIn brings enhanced automation and personalization to Office applications like Outlook, Word, PowerPoint, and Teams. In Outlook, contacts are streamlined by automatically adding colleagues from LinkedIn, while relevant connections can be suggested for meetings or email threads based on expertise. LinkedIn profiles are seamlessly displayed within Outlook emails, providing valuable context. In Word and PowerPoint, Linkedln skills and experiences are effortlessly incorporated into resumes or professional bios with a click. Teams benefit from automatically created calendars and schedules, along with suggested team members based on project goals and Linkedln connections. Dynamic functionality includes intelligent search across Office and Linkedln data, real-time updates on colleagues' activities, and personalized news feeds tailored to Linkedln profiles and activities.

However, as these functionalities rely on accessing Linkedln data, data security and privacy become paramount. Transparency, user control over data sharing, and robust security measures are essential to ensure trustworthiness and protect user privacy. This emphasis on responsible data handling underscores the importance of maintaining user confidence in the integrated experience.

Current Situation:

- The deal was approved with the aforementioned safeguards in place. The final deal involved concessions from Microsoft, including data privacy commitments and limitations on data sharing.
- The acquisition was ultimately approved by most authorities, although some concerns remain about its long-term implications for competition and data privacy.
- This case exactly highlights the complex challenges of balancing innovation, competition, and data privacy in the digital age.
- However, user privacy concerns regarding data collection and potential future uses remain a point of discussion.
  Hence, Future acquisitions of similar scope are likely to face similar scrutiny and potential regulatory hurdles.

Regulatory Scrutiny:

- The EU and other regulatory bodies reviewed the deal to ensure it didn't stifle competition or violate user privacy.

- Microsoft addressed these concerns by:
    - Committing to strong data separation between LinkedIn and Microsoft products.
    - Limiting data sharing for specific purposes like improving search functionality across platforms (e.g., suggesting relevant LinkedIn connections in Microsoft Outlook).
    - Providing clear user controls over data sharing and privacy settings.[36] [37] [38]

IV. Facebook (Meta) and Data Practices: A Tangle of Privacy and Competition Concerns:

Facebook, now under the parent company Meta, has a long and complex history with data privacy concerns and has faced various legal challenges from the Federal Trade Commission (FTC) and other regulators, focusing on both data privacy and competition issues. Here's a breakdown in simple pointers:

The Issue:

i) Facebook collects a vast amount of user data, including browsing habits, likes, demographic information, and even private messages (in some cases).

ii) The concern is how Facebook uses this data and whether users have sufficient control over it.[39]

Privacy Scandals:

- Cambridge Analytica (2018): A data analytics firm improperly accessed data from millions of Facebook profiles without user consent, raising questions about data security and user control.
- EU Fines (2017, 2022): Facebook (Meta) was fined by the EU for privacy violations related to data handling and transparency.
- Opaque Practices: Critics argue that Facebook's data practices and privacy settings are complex and confusing, making it difficult for users to understand how their data is used. Hence, Data privacy remains a key concern, with questions about how Facebook collects, uses, and shares user data.
- The CCI is currently reviewing the privacy policy of WhatsApp, another Meta-owned application, which shares users' data with Facebook without providing a meaningful opt-out option.

[36] Ram Bhadra, "LinkedIn: A Case Study into How Tech Giants Like Microsoft Abuse Their Dominant Market Position to Create Unlawful Monopolies in Emerging Industries," 13 Hastings Sci. & Tech. L.J. 3 (2022).
[37] The Verge, "Microsoft ordered to let third parties scrape LinkedIn data," August 15, 2017.
[38] Portia Cerny on LinkedIn, "Microsoft offers legal protection for users," LinkedIn post.
[39] Alyssa Newcomb, "Timeline: Facebook's Privacy Issues and Its Responses", NBC News (Mar. 26, 2018), https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651.

Volume 32, May 2024 ISSN 2581-5504

- Another Meta Platform, Threads' unprecedented growth and its reliance on Meta's existing user base pose both regulatory and privacy challenges in India's digital landscape.

Potential Harm to Competition:

- Instagram Acquisition (2012): Facebook acquired Instagram, a rising media-sharing platform, raising concerns about stifling competition.
- WhatsApp Acquisition (2014): Facebook bought messaging app WhatsApp, further amplifying competition concerns.
- Meta Platforms, which owns Facebook, Instagram, and WhatsApp, recently launched Threads as a rival to Twitter.
    - Within just five days, Threads amassed a staggering 100 million new users-a feat that took Twitter over five years to achieve.
    - Threads leverages Meta's 2.35 billion-strong Instagram user base to create momentum for itself.
    - Unlike other alternative micro-blogging platforms, Threads requires an Instagram account to access.
    - The rapid growth of Threads raises questions for Indian competition law. While it provides Indian users with an alternative to the chaotic Musk-era Twitter, the manner in which Meta achieved this scale of growth warrants scrutiny by the Competition Commission of India (CCI).
- Antitrust Lawsuits: The FTC and several states filed lawsuits against Facebook, alleging that these acquisitions were anti-competitive, aimed at eliminating potential rivals.
- The lawsuits are ongoing, with Facebook defending its acquisitions as beneficial for users and denying any intent to harm competition.[40]

Meta's Response:

- Privacy Controls: Meta has updated its privacy settings to give users more control over their data.
- Transparency Efforts: They've made attempts to be more transparent about data collection and usage.
- Focus on Aggregation: Meta emphasizes using data in aggregate for advertising purposes, not personally identifying individual users.[41]

Current Situation:

[40] Gilad Edelman, "Competition Is at the Heart of Facebook's Privacy Problem," Wired (Oct. 9, 2019), https://www.wired.com/story/competition-is-at-the-heart-of-facebooks-privacy-problem/.
[41] Financial Express, "CCI Must Watch Meta's Threads: Unprecedented Growth Raises Concerns over Privacy and Competition Law in India," Financial Express (Aug. 25, 2022), https://www.financialexpress.com/opinion/cci-must-watch-metas-threads-unprecedented-growth-raises-concerns-over-privacy-and-competition-law-in-india/3192998/.

Volume 32, May 2024 ISSN 2581-5504

- Ongoing Scrutiny: Despite Meta's efforts, data privacy concerns persist.
- Regulatory Landscape: New data privacy regulations around the world are putting pressure on Meta to improve its data practices.
- Focus on the Future: Meta is investing in technologies like the Metaverse that raise new questions about data collection and privacy in virtual worlds.

This saga about Facebook's data and competition and data privacy issues is far from over. As these cases unfold, the future of user privacy and fair competition in the digital world will be shaped by regulatory decisions and court rulings.[42] [43]

Microsoft's integration of LinkedIn raised concerns about data privacy and market dominance, as the acquisition allowed Microsoft to access vast amounts of user data.

Similarly, Facebook's (Meta's) data practices, including the Cambridge Analytica scandal, have led to scrutiny over its handling of user data and acquisitions of potential rivals like Instagram and WhatsApp.

These cases underscore the challenges of balancing innovation, competition, and data privacy in the tech industry, as regulators grapple with how to ensure consumer protection without stifling innovation.

V. Baidu's Monopoly- Hudong vs. Baidu: A Search for Fairness in the Chinese Web (2008)

In 2008, a battle royale erupted in the Chinese web, pitting two online encyclopedia giants against each other: Hudong, the established player, and Baidu, the rising search engine star.

Hudong accused Baidu of manipulating search results and unfairly suppressing their entries, a David vs. Goliath fight with significant implications for competition and internet freedom.

Act I: The Accusation (2008)

Hudong threw the first stone, complaining that Baidu search results consistently favored its own Baike encyclopedia over Hudong's entries. They presented evidence of manipulated rankings, suggesting Baidu used its dominant search engine position to stifle competition and steer users towards Baike.

Act II: The Investigation and the Showdown (2008-2009)

The Chinese Ministry of Commerce stepped in, launching an investigation into the allegations. While the investigation remained confidential, the public watched with bated breath as both sides argued their cases. Hudong emphasized the importance of fair competition and user

[42] Brandon Vigliarolo, "Facebook Data Privacy Scandal: A Cheat Sheet", TechRepublic (Apr. 10, 2018), https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/.
[43] Alessandro Acquisti & Ralph Gross, "Privacy and Rationality in Individual Decision Making", 9 IEEE Security & Privacy 26 (2011), https://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf.

Volume 32, May 2024 ISSN 2581-5504

choice, while Baidu defended its algorithms, claiming they were objective and based on relevance, not favoritism.

Act IlI: The Verdict and the Aftershocks (2009-Present)

The Ministry of Commerce ultimately reached a decision in 2009, but the official verdict remained unpublished. Sources suggest Baidu received a minor reprimand for "unlawful competition," but no significant fines or penalties were imposed.

Here's a breakdown of the key issues in hand:

The Concerns:

- Search Manipulation:
  - Accusations: Baidu has been accused of manipulating search results to favor its own products and services, or those of companies that pay for preferential treatment. This could limit user choice and affect competition.
  - Examples:
    - Prioritizing its own Baike encyclopedia over competitors like Hudong in search results.
    - Demoting or blocking links to rival companies' websites.
- Advertising Monopoly:
  - Accusations: Baidu controls a large share of the online advertising market in China, leading to concerns about unfair pricing and practices that could harm smaller advertisers.
  - Examples:
    - Requiring high minimum ad spends.
    - Restricting access to data and analytics tools for smaller advertisers.
- Other Anti-Competitive Practices: Baidu's exclusive deals like forcing companies to use its services exclusively to gain better search rankings hindering competition from other search engines.

Examples of Cases:

- 2009: Qmyy.com, a video-sharing platform, sued Baidu for allegedly blocking its web pages from search results.
- 2016: The State Administration for Industry and Commerce (SAIC), a Chinese regulatory body, investigated Baidu on suspicion of anti-competitive practices. The outcome of this investigation isn't publicly available.

Aftermath:

- Hudong vs. Baidu highlighted the delicate balance between search engine algorithms and fair competition. While the official verdict remains shrouded in secrecy, the case opened a vital discussion about search neutrality and potential manipulation by dominant platforms.

- The lack of a clear and public outcome left many unsatisfied, leaving questions about Baidu's practices and the effectiveness of Chinese antitrust enforcements in the tech sector.
- Despite the inconclusive verdict, the case marked a turning point in China's online landscape. It raised awareness about the power of search engines and their potential influence on users' information access.
- Hudong continued to operate, but its market share continued to decline in the face of Baidu's dominance. The case became a symbol of the challenges faced by smaller players in China's internet ecosystem.
  [44] [45] [46]

Personal Opinion

The rise of AI and the dominance of tech giants have brought forth a complex landscape where the benefits of innovation and efficiency must be carefully balanced against the risks of anti-competitive practices and data privacy violations. As AI technologies continue to evolve, enabling data-driven insights and personalized services, it is imperative to establish robust regulatory frameworks that promote fair competition while safeguarding individual privacy rights.

Collaboration between competition authorities and data protection bodies is crucial in navigating this intricate terrain. Clear and comprehensive data protection laws must be swiftly enacted, providing guidelines for responsible data collection, processing, and sharing practices. These laws should empower users with greater control over their personal information and facilitate data portability, fostering a more competitive digital ecosystem.

Moreover, competition law must adapt to the realities of the data-driven economy, recognizing data as a critical asset and addressing potential abuses of market power through the exploitation of data advantages. Regulatory bodies should closely scrutinize the practices of tech giants, ensuring transparency in algorithmic decision-making processes and preventing the unfair leveraging of user data to stifle competition or entrench monopolistic positions.

Interoperability emerges as a powerful tool in this context, enabling seamless data exchange and promoting innovation by lowering barriers to entry for new market participants. Mandating interoperability requirements and facilitating data sharing can foster a more level playing field, empowering consumers with greater choice and mitigating the risks of market foreclosure.

Ultimately, the path forward lies in striking a delicate balance between harnessing the transformative potential of AI while upholding the principles of fair competition and data privacy. Regulatory bodies, policymakers, and tech giants must collaborate to create an

[44] Jones Day, "Antitrust Alert: Second Chinese 'Dominance' Decision Issued Under the China Anti-Monopoly Law," January 2010.
[45] Digital Trends, "Panguso search, Baidu monopoly investigation leave Chinese Internet at crossroads," February 23, 2011.
[46] China Daily, "Baidu accused of abusing dominant position," February 23, 2011.

Volume 32, May 2024 ISSN 2581-5504

environment that nurtures innovation while safeguarding consumer welfare and individual rights in the digital age.

Conclusion

In conclusion, the significance of competition law and data privacy regulations cannot be overstated in today's digital economy. Competition law plays a crucial role in promoting fair market practices, fostering innovation, and protecting consumer welfare, while data privacy regulations are essential for safeguarding personal information and preserving individual rights. In India, the intersection of these two legal frameworks is evident in the role of the Competition Commission of India (CCI) in regulating privacy concerns within the digital realm.

The CCl's understanding of competition law extends to include privacy as a non-price parameter, highlighting the importance of data privacy in maintaining fair market practices. The enactment of the Digital Personal Data Protection Act (DPDPA) further underscores the need to balance individual rights with data processing activities. However, navigating spaces where privacy and competition law intersect poses challenges, as demonstrated in cases like WhatsApp's data-sharing practices with Facebook.

While privacy infringements may be considered in competition law analysis, evidence of misconduct that undermines fair competition is essential for establishing a violation. It's crucial to maintain a clear distinction between competition law and data protection regulations, ensuring each framework fulfils its objectives without conflating their purposes. This analytical independence enhances predictability, upholds the rule of law, and contributes to a transparent business environment.

Effective enforcement and coordination between competition law and data privacy regulations are vital for creating an environment where businesses can thrive while respecting individuals' rights and privacy. This holds true within the context of Indian laws, where regulatory authorities must balance the need for innovation and competition with the protection of personal data and consumer welfare. By striking this balance, India can foster a digital economy that is both competitive and respectful of privacy rights.

References

1. Chui, M., Hazan, E., Roberts, R., Singla, A., Smaje, K., Sukharevsky, A., Yee, L., & Zemmel, R. (2023). The economic potential of generative AI: The next productivity frontier. In McKinsey & Company. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier

2. Dellemijn, M. (2023, October 5). How businesses can ethically embrace artificial Intelligence. Forbes.

https://www.forbes.com/sites/forbesbusinesscouncil/2023/05/12/how-businesses-can-ethically-embrace-artificial-intelligence/?sh=4058588520a3

3. Naik, N., Hameed, B. M. Z., Shetty, D. K., Swain, D., Shah, M., Paul, R., Aggarwal, K., Ibrahim, S., Patil, V., Smriti, K., Shetty, S., Prasad, B., Chłosta, P., & Somani, B. (2022). Legal and ethical consideration in artificial intelligence in healthcare: Who takes responsibility? Frontiers in Surgery, 9. https://doi.org/10.3389/fsurg.2022.862322.

4. Amlegals, D. O. (2023, January 4). Interplay between Data Protection and Competition Law. Law Firm in Ahmedabad. https://amlegals.com/interplay-between-data-protection-and-competition-law/ 5. Panel for the Future of Science and Technology: EPRS | European Parliamentary Research Service, ISBN: 978-92-846-6771-0, Law, State and Telecommunications Review. (2021, September 7). AI Training Datasets & Article 14 GDPR: A Risk Assessment for the Proportionality Exemption of the Obligation to Provide Information.

5. Marr, B. (2024, February 20). The 15 biggest risks of artificial intelligence. Forbes. https://www.forbes.com/sites/bernardmarr/2023/06/02/the-15-biggest-risks-of-artificial-intelligence/?sh=58deb4852706

6. NITI Aayog. (2022). India's Booming gig and platform Economy: Perspectives and Recommendations on the Future of Work. (n.d.).

7. EduZone: International Peer Reviewed/Refereed Multidisciplinary Journal. (n.d.). https://www.eduzonejournal.com/index.php/eiprmj

8. Online, E. (2023, April 25). AI and Privacy: The privacy concerns surrounding AI, its potential impact on personal data. The Economic Times. https://economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy-concerns-surrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cms?from=mdr

9. Gartner, 25, March 2024, https://www.gartner.com/en/newsroom/press-releases/2020-02-25-gartner-says-over-40-percent-of-privacy-compliance-technology-will-rely-on-artificial-intelligence-in-the-next-three-years-

10. ,Ramanpreet Kaur Artificial intelligence for Cybersecurity: Literature review and Future Research Directions, Information Fusion Journal. (n.d.). Information Fusion Journal., Volume 97, Year-2023, Issn- 1566-2535, 25 March, 2024.

Volume 32, May 2024 ISSN 2581-5504

11. Managing the competition law risks of AI. (n.d.). https://www.dentons.com/en/insights/articles/2023/november/17/managing-the-competition-law-risks-of-ai

12. Report of the Committee on Digital Competition Law, Ministry of Corporate Affairs Government of India, https://www.cci.gov.in/images/antitrustorder/en/142019-and-0120201652511256.pdf March 24, 2024

13. Ghosh, S. (2021, May 30). The biggest data breaches in India. CSO Online. https://www.csoonline.com/article/569325/the-biggest-data-breaches-in-india.html

14. ETHICS: IT'S RELATION WITH INDIAN SCRIPTURES AND BUSINESS. (n.d.). International Journal of Core Engineering & Management (IJCEM).

15. Competition Law And Privacy: An Opinion on The Future of a Complicated Relationship (June 08, 2022), https://competitionlawblog.kluwercompetitionlaw.com/2022/06/08/competition-law-and-privacy-an-opinion-on-the-future-of-a-complicated-relationship/, Kluwer Competition Law Blog- March 25, 2024

16. Data portability, interoperability and competition. (n.d.). Oced. https://www.oecd.org/daf/competition/data-portability-interoperability-and-competition.htm

17. "Interoperability of Digital Platforms May Raise User Security Risks," Business Standard (February 14, 2024), https://www.business-standard.com/technology/tech-news/interoperability-of-digital-platforms-may-raise-user-security-risks-124021400916_1.html.

18. Harvard Business Review, "Understanding the Tradeoffs of the Amazon Antitrust Case," January 11, 2024, https://hbr.org/2024/01/understanding-the-tradeoffs-of-the-amazon-antitrust-case.

19. The New York Times, "Amazon Set to Face Antitrust Charges in European Union," June 11, 2020, https://www.nytimes.com/2020/06/11/technology/amazon-antitrust-european-union.html.

20. SSRN, "Google v Commission (Google Shopping): A Case Summary," November 29, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3965639.

Volume 32, May 2024 ISSN 2581-5504

21. European Commission, "CASE AT.39740 Google Search (Shopping) ANTITRUST PROCEDURE," June 27, 2017, https://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf.

22. Kluwer Competition Law Blog, "Google Shopping: The General Court takes its position," November 15, 2021.

23. Data portability, interoperability and competition. (n.d.). Oced. https://www.oecd.org/daf/competition/data-portability-interoperability-and-competition.htm

24. Reuters, "Google loses challenge against EU antitrust decision, other probes loom," September 14, 2022, https://www.reuters.com/technology/eu-courts-wed-ruling-record-44-bln-google-fine-may-set-precedent-2022-09-14/.

25. Belloso, N. M. (2021). Google v Commission (Google Shopping): A Case Summary. Social Science Research Network. https://doi.org/10.2139/ssrn.3965639.

26. 34. *Yale Law Journal: Vol. 132.* Yale Law Journal, 2022. https://www.yalelawjournal.org/files/Volume132StyleGuiderev.2022.11.02_nqty59xo.pdf.

27. Lemley, Mark A., and Shubha Ghosh. *Antitrust Law: Cases and Materials.* Foundation Press, 2019. https://ir.law.utk.edu/cgi/viewcontent.cgi?article=1751&context=utklaw_facpubs.

28. Ram Bhadra, "LinkedIn: A Case Study into How Tech Giants Like Microsoft Abuse Their Dominant Market Position to Create Unlawful Monopolies in Emerging Industries," 13 Hastings Sci. & Tech. L.J. 3 (2022).

29. The Verge, "Microsoft ordered to let third parties scrape LinkedIn data," August 15, 2017.

30. Portia Cerny on LinkedIn, "Microsoft offers legal protection for users," LinkedIn post.

31. Alyssa Newcomb, "Timeline: Facebook's Privacy Issues and Its Responses", NBC News (Mar. 26, 2018), https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651

32. Gilad Edelman, "Competition Is at the Heart of Facebook's Privacy Problem," Wired (Oct. 9, 2019), https://www.wired.com/story/competition-is-at-the-heart-of-facebooks-privacy-problem/.

Volume 32, May 2024 ISSN 2581-5504

33. Bose, A. (2023, July 31). CCI must watch Meta's Threads; unprecedented growth raises concerns over privacy and competition law in India. Financial Express. https://www.financialexpress.com/opinion/cci-must-watch-metas-threads-unprecedented-growth-raises-concerns-over-privacy-and-competition-law-in-india/3192998/

34. Brandon Vigliarolo, "Facebook Data Privacy Scandal: A Cheat Sheet", TechRepublic (Apr. 10, 2018), https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/.

35. Alessandro Acquisti & Ralph Gross, "Privacy and Rationality in Individual Decision Making", 9 IEEE Security & Privacy 26 (2011), https://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf.

36. Jones Day, "Antitrust Alert: Second Chinese 'Dominance' Decision Issued Under the China Anti-Monopoly Law," January 2010.

37. Digital Trends, "Panguso search, Baidu monopoly investigation leave Chinese Internet at crossroads," February 23, 2011.

38. China Daily, "Baidu accused of abusing dominant position," February 23, 2011.