FROM GROUND REALITY TO THEORY: HOW DATA PRIVACY HAS USED ITSELF A YARDSTICK FOR COMPETITION LAW

Aashka Vyas, O.P. Jindal Global University, Jindal Global Law School

ABSTRACT

Antitrust theory sees data privacy as benefiting from competition; however, this paper argues that such a stance overlooks the complex interplay between antitrust principles and data privacy concerns. In reality, data privacy has evolved into its own legal realm over the past twenty-five years. Consequently, it can intersect and sometimes clash with antitrust, akin to how intellectual property or consumer protection laws have in the past. This paper sheds light on the intricate dynamics at the junction of antitrust and data privacy, offering insights into the emerging tensions. It provides a descriptive, historical, and comparative analysis of the conflicts arising between these legal spheres in the digital economy, where data accessibility can simultaneously drive competition and compromise privacy. Furthermore, the paper introduces a fresh approach to assess conflicting interests between data privacy and competition, one aimed at balancing the objectives of both legal domains.

Keywords: data privacy, antitrust, competition, interface, big tech, digital market, control over data, data protection.

Introduction

Antitrust regulations and data privacy laws wield considerable influence over the handling of digital data. They are increasingly focused on regulating the activities of major digital platforms such as Facebook, Google, Apple, and Amazon. These companies are frequent targets of enforcement actions by the Federal Trade Commission (**"FTC"**) for data privacy violations, as well as facing stringent regulations under the European data protection framework. As India has now commenced to theorize this new convergence of digital data privacy and antitrust law by increasing the ambit of Digital Personal Data Protection Act (**"DPDPA"**), 2023[1] and also through the newly passed draft Digital Competition Bill (**"DCB"**), 2024[2], it is imperative to understand the new antitrust/data privacy law interface in India stemming from the concepts prevalent in the United States (**"US"**) and the European Union (**"EU"**).

Part I of this paper assesses how and why the FTC came to dominate the enforcement of privacy policies through the case of FTC v. Amazon[3] that was one of the defining cases establishing and determining broader antitrust reform movement. Part II of this paper encompasses the key outcome from the ruling issued by the Court of Justice of the European Union (**"CJEU"**) in the Meta Platforms case on July 4, 2023, that competition authorities have the authority to recognize a breach of data protection regulations when it is essential for establishing an abuse of dominance under competition laws. Part III explores the changing digital terrain of India, characterized by a notable increase in data utilization and technological progress and tracing the path from the Information Technology Act, 2011 (**"IT Act"**)[4] to the DPDPA, and the introduction of the DCB to delve further into the complex convergence of data protection, competition law, and the hurdles posed by major tech companies in influencing India's digital trajectory.

Amazon's Antitrust Anomaly: A Crucial Test for the FTC and the law for Control over Data

Originally established in 1914, the FTC was created to ensure fair competition within the market. Over the years, its authority has expanded gradually, and significant milestone was the enactment of the Wheeler-Lea Amendment to the FTC Act[5], which broadened the FTC's

[1] Digital Personal Data Protection Act (DPDPA), Acts of Parliament, 2023 (India).
[2] Digital Competition Bill, Report of the Committee on Digital Competition Law, Ministry of Corporate Affairs, 2024 (India).
[3] Federal Trade Commission v. Amazon.com Inc, 2:23-cv-01495, (W.D. Wash.).
[4] Information Technology Act (IT Act), Acts of Parliament, 2011 (India).
[5] Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (US).

jurisdiction to include the prohibition of *"unfair or deceptive acts or practices"* alongside *"unfair methods of competition"*. This empowered the FTC to directly protect consumers in addition to its antitrust efforts. Since the adoption of Section 5[6] of the FTC Act, the FTC has actively pursued violations of various antitrust and consumer protection laws, including cases involving false advertising and unsafe products and subsequently consumer privacy issues. The FTC's authority for privacy enforcement primarily stems from Section 5, which prohibits *"unfair or deceptive acts or practices in or affecting commerce"*. An act or practice is considered 'unfair or deceptive' if it involves a material misrepresentation, omission, or practice likely to mislead a reasonable consumer, or if it causes substantial harm to consumers that is not reasonably avoidable and is not outweighed by benefits to consumers or competition. Therefore, when enforcing Section 5, the FTC can identify privacy violations based on either deceptive or unfair trade practices.[7] Currently, the FTC is seen as the primary federal body responsible for safeguarding data. This role, akin to that of a data protection authority found in many other countries' privacy laws, grants the FTC the authority to enforce privacy regulations.

On September 26, 2023, the FTC and 17 State Attorneys General (collectively referred to as "the agencies") filed an eagerly awaited complaint against Amazon, alleging breaches of Section 2[8] of the Sherman Act, Section 5 of the FTC Act, and various state laws related to competition and consumer protection. The allegations include claims that Amazon had a monopoly in the online superstore and online marketplace services markets, engaged in unfair competition through its actions and a pricing algorithm named "Project Nessie", and violated state competition and consumer protection laws in several states including Connecticut, Maine, Maryland, Michigan, Nevada, New Jersey, New York, Oklahoma, Oregon, Pennsylvania, Rhode Island, and Wisconsin.[9] Amazon responded staunchly in a widely circulated public statement, defending its practices and arguing that they are beneficial and protective of consumers, as well as fostering competition. The long-awaited lawsuit arrives over two years after Lina Khan assumed the role of FTC chair, and more than six years after she authored a student note criticizing Amazon's operations. In her article "Amazon's Antitrust Paradox"[10], Lina Khan argued that current antitrust laws fail to effectively identify certain types of

[6] Section 5 of the FTC Act, 15 U.S.C. § 45 (2006).
[7] Daniel J. Solove & Woodrow Hartzog, *The FTC and The New Common Law of Privacy*, 114:583 CLR 583, 598-599 (2014).
[8] Section 2 of the Sherman Act, 15 U.S.C. § 2 (1970).
[9] Jung Kim & Arianna Chen, FTC's Amazon Antitrust Lawsuit from A to Z, AMERICAN BAR ASSOCIATION (Mar. 27, 2024), https://www.americanbar.org/groups/antitrust_law/resources/newsletters/ftc-amazon-antitrust-lawsuit/.
[10] Lina M. Khan, Amazon's Antitrust Paradox, 126:710 TYLJ 710, 2017.

anticompetitive behaviour in platform and data-driven markets, using Amazon as a prime example. In her opinion, the current framework fails to grasp the intricacies of the platform business model, where scale is prioritized over short-term profit, making predatory pricing a strategic choice. Moreover, she argues that vertical integration and control over data by platforms can lead to new forms of anticompetitive behaviour. She asserts that the failure to recognize Amazon's actions as anticompetitive has allowed it to dominate multiple markets. Therefore, she emphasized the necessity of reforming antitrust regulations to address these shortcomings.

Amazon's dominance in the online platform realm stems from two key components of its business strategy: its willingness to incur losses and invest aggressively, prioritizing growth over immediate profits, and its integration across multiple sectors. These strategic elements are not only significant individually but also deeply interconnected and thus Amazon's expansion into various areas often involves sacrificing short-term profits. This strategy, prioritizing market share over immediate profits, challenges the rational, profit-driven model advocated by the Chicago School. Numerous facets of Amazon's actions have faced scrutiny in the media, policy discussions, and academic literature. However, for the present discussion and examination, I narrow down one particular concern highlighted by Lina Khan in her note which is Amazon's "control over data". Khan contended that the existing antitrust framework overlooks the significance of concentrated control over data, which enables a digital platform to skew a market in its own favour.[11]She asserted that Amazon exploits its position as a dominant platform, and its capacity to amass extensive data to gain leverage over sellers operating within its Marketplace. Amazon appears to utilize its Marketplace as an extensive testing ground for identifying and assessing new products for sale, while also exerting greater control over pricing. Specifically, reports indicate that Amazon leverages sales data from external merchants to inform its purchasing decisions, enabling it to undercut competitors on pricing and prioritize its own items for prominent placement in search results. For example, with respect to a product Pillow Pets, plush animal pillows resembling NFL mascots, which a third-party seller offered through Amazon's platform, the merchant initially experienced robust sales of up to one hundred pillows daily. However, just before the holiday season, the merchant observed that Amazon itself began offering identical Pillow Pets at the same price, while prominently featuring its own products on the site. Consequently, the merchant's sales

[11] *Id.* at 783.

plummeted to twenty pillows per day.[12] While it is accurate that traditional brick-and-mortar retailers occasionally launch their own brands and may rely on competitors' sales data to inform their product offerings, Amazon's approach stands out due to the sheer scale and complexity of the data it gathers. Unlike physical stores, which typically only have access to data on actual purchases, Amazon tracks a myriad of additional data such as what shoppers are searching for but fail to locate, which items they frequently return to, what they add to their shopping carts, and even where their cursor hovers on the screen.[13]

In the realm of competition policy, a critical consideration regarding online platform markets is their tendency toward "winner-takes-all" dynamics. This trend predominantly arises from the influence of control over data that perpetuate over time. By accessing consumer data, platforms can enhance service customization and gauge market demand more effectively. Additionally, operating across various markets may allow a company to leverage data acquired from one sector to benefit another business sector which Amazon usually does with its Marketplace data to bolster its retail sales. Moreover, control over data can streamline the entry of dominant platforms into new markets. For instance, recent reports indicate that Amazon is contemplating a significant expansion into the advertising sector by utilizing the vast pool of shopping data amassed from its extensive e-commerce operations. In essence, control over data also functions as a barrier to entry. As online platforms continue to play a larger role in both communication and commerce, it is imperative to update antitrust laws accordingly. This becomes even more crucial given the potential for concentrated control over data to breed new forms of anticompetitive behaviour.

CJEU's interpretation of competition law rules by welcoming data protection standards through the Meta Platforms Case

As we reckoned Amazon's Antitrust Paradox through FTC's lens that the current antitrust framework has not fully acknowledged companies wielding significant control over data can systematically sway a market in their favour, leading to substantial reshaping of the sector. In contrast to U.S. antitrust authorities (FTC), European counterparts actively investigate the potential anticompetitive effects of concentrated control over data because of the existence of an established data protection framework in the EU called the General Data Protection

[12] *Id.* at 781.
[13] *Id.* at 782.

Regulation (**"GDPR"**)[14]. In a strongly worded decision on July 4, 2023[15], the CJEU responded to the inquiries from the Higher Regional Court in Düsseldorf regarding the validity of the approach taken by the German Federal Cartel Office (Bundeskartellamt) in its 2019 competition ruling[16] against Facebook (now Meta) with EU law. The Bundeskartellamt had previously held Meta accountable under German competition regulations for imposing unfair terms and conditions, assessed based on the standards outlined in the GDPR. In its preliminary ruling, the CJEU echoed the Opinion of Advocate General Rantos[17] and endorsed the Bundeskartellamt's use of GDPR data protection rules to establish abuse of dominance under competition law. Additionally, the CJEU clarified the interpretation of GDPR legal provisions governing personal data processing activities by big tech giants like Meta and provided a framework to assist competition and data protection authorities in coordinating cases where GDPR regulations are relevant for assessing compliance with competition law.

In February 2019, the Bundeskartellamt had issued its competition ruling against Meta stating that Meta held a dominant position in the social network market and was accused of abusing this dominance. The alleged abuse involved compelling users to consent to the combination of data collected from Meta's various services and third-party sources as a condition for accessing the Facebook social network. The Bundeskartellamt concluded that Meta lacked a legitimate legal basis under the GDPR for this data combination practice, constituting an exploitative abuse under Section 19 (1) of the German Competition Act (Gesetz gegen Wettbewerbsbeschränkungen, GWB).[18] The case reached the EU level through a preliminary reference to the CJEU from the Higher Regional Court in Düsseldorf during the substantive proceedings. The CJEU unequivocally affirms the ability of national competition authorities to scrutinize the alignment of personal data processing with the GDPR when assessing the presence of an abuse of dominance. While recognizing the distinct roles and responsibilities of data protection and competition authorities, the CJEU emphasizes that the GDPR does not prohibit national competition authorities from identifying GDPR violations in the course of

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.
[15] Case C-252/21 *Meta Platforms v. Bundeskartellamt*, EU:C:2023:537.
[16] Case B6-22/16, *Facebook – exploitative business terms*, 6 February. 2019, www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5.
[17] Opinion of Advocate General Rantos in Case C-252/21 *Meta Platforms v. Bundeskartellamt*, EU:C:2022:704.
[18] Inge Graef, Meta platforms: How the CJEU leaves competition and data protection authorities with an assignment, 30 (3) MAASTRICHT JOURNAL OF EUROPEAN AND COMPARATIVE LAW 325, (2023).

their duties.[19] According to the CJEU, compliance with the GDPR can serve as a crucial factor in determining whether a conduct conforms to competition rules. Moreover, the CJEU highlights that access to personal data has emerged as a significant competitive parameter in the digital economy. Therefore, disregarding GDPR regulations from the legal framework considered by competition authorities in abuse of dominance cases would ignore the evolving economic landscape and risk undermining the effectiveness of competition law in the EU.[20] Another notable aspect of the judgment is where the CJEU lays out a broad framework for collaboration between data protection and competition authorities, filling the gap left by the absence of specific regulations in the EU law. Leveraging the principle of sincere cooperation enshrined in Article 4 (3) of the Treaty on the European Union, the CJEU elucidates that competition authorities must engage in genuine consultation and cooperation with data protection authorities to ensure that the provisions of GDPR are complied with.[21] In addition to the GDPR, the Digital Markets Act (**"DMA"**) mandates that gatekeepers providing core platform services must refrain from merging personal data across services unless the end user has provided consent as defined by the GDPR.

The assertive language employed by the CJEU suggests that it views the Meta Platforms case as a clear instance where a competition authority has appropriately intervened, following coordination with pertinent data protection authorities, against behaviour that likely breaches the GDPR. Beyond the specifics of this case, the CJEU has clarified that data protection regulations can play a role for competition authorities in determining instances of abuse of dominance. Moreover, dominance itself can be a factor in assessing the validity of consent under the GDPR. By interpreting all legal bases for personal data processing, the CJEU has provided valuable clarifications regarding the GDPR's scope, potentially aiding data protection authorities in enforcing compliance more effectively in the future. While the CJEU has brought clarity regarding the legality of Meta's personal data processing under the GDPR, and the DMA has extended the same requirement to other gatekeepers, future cases at the intersection of data protection and competition law may not be as straightforward. These cases could involve less pronounced dominance by the data controller or less clear-cut issues with its data processing activities. Therefore, while the CJEU has paved the way for further alignment between these

[19] Case C-252/21 Meta Platforms v. Bundeskartellamt, para. 43–44.
[20] *Id.* at para. 51.
[21] *Id.* at para. 53-54.

legal realms, it also underscores the need for competition and data protection authorities to coordinate their respective competencies and interpretations of the law going forward.

Evolution and Application of the interface between Competition Law and Data Privacy in India

A consensus is forming among competition regulators worldwide that in markets fuelled by data-driven business models, the concepts of antitrust and data protection regulations intersect. India, experiencing rapid growth, has emerged as a fertile ground for expansive digital market segments, fuelling exponential growth in its digital landscape. However, this surge has brought forth a myriad of complexities, particularly surrounding large digital enterprises, resulting in a surge of unfair trade practices, consumer rights violations, and biased policies. With the proliferation of commercial activities in the digital sphere, there is a pressing need to implement pre-emptive safeguards, superseding the current measures in enforcing competition laws. Although the IT Act aimed to tackle fundamental issues initially, it struggled to keep pace with the rapid and evolving technological landscape. Data swiftly transformed into a valuable asset, utilized by major entities to gauge economic prowess through the monetization of user-collected data- tracking consumer preferences, shaping consumer behaviour, and beyond. India's data protection legislation originated from the landmark Supreme Court ruling in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[22]. Subsequently, a Committee led by a former Supreme Court judge was tasked with crafting a comprehensive framework, culminating in the production of a report and two draft legislations. The current iteration of the Data Protection Act, known as the DPDPA, represents a notably altered and somewhat belated version of the envisioned data protection law. Simultaneously, there occurred a significant shift in the types of cases handled by the Competition Commission of India (**"CCI"**). Initially, the CCI did not regard online marketplaces or platforms as distinct entities from their offline counterparts. Furthermore, it had not yet recognized markets like the Google Play Store or Amazon as separate and self-contained ecosystems. However, by 2018, in the case of *All India Online Vendors Association (**"AIOVA"**) v. Flipkart*[23], the CCI had notably refined its approach to delineating digital markets. In this instance, the CCI identified Flipkart as a distinct online platform, classifying its market as "services provided by online marketplaces for selling goods in India", rather than adopting the broader definition sought by Flipkart, which encompassed a

[22] Justice K.S. Puttaswamy (Retd.) v. Union of India (Right to Privacy Case), (2017) 10 SCC 1.

[23] All India Online Vendors Association ("AIOVA") v. Flipkart, Case No. 20 of 2018.

"pan-India market for retail or B2C, including online and offline channels of distribution". The case centred on allegations that Flipkart exploited its dominant position within its marketplace to favour its private labels over those of competing sellers. However, the case was dismissed at the outset, as the CCI ruled that with a competitor like Amazon present, Flipkart could not be deemed a dominant platform. The Competition Law Review Committee Report of 2019[24] solidified the trajectory the CCI would ultimately follow. Although the report did not explicitly propose changes to the legal definition of relevant markets to accommodate the unique impacts of digital platforms, the CCI has indicated that it will now treat offline and online markets as distinct entities. Before the Competition Law Review Committee Report of 2019, the CCI had not played an active role in regulating digital markets. However, in 2020, the CCI recognized privacy as a non-price factor influencing competition, as outlined in a market study report on the telecom sector (Competition Commission of India, 2021)[25].

In 2016[26], the CCI initially dismissed allegations against WhatsApp, a dominant player in the market, regarding excessive data collection. However, in January 2021, it adopted a more nuanced approach by invoking its powers under section 19(1) to initiate a *suo moto* investigation against WhatsApp and Facebook.[27] This decision came in response to WhatsApp's updated privacy policy, which mandated data sharing with Facebook. Unlike its stance in 2016, the CCI acknowledged the high switching costs and the opaque language of the policy, raising concerns about the impact on consumers. The CCI criticized WhatsApp's "take it or leave it" approach, highlighting the lack of choice for users to object or opt-out of specific data sharing terms. Importantly, the CCI recognized that the reduction in consumer data protection and loss of control over personalized data could be construed as a decrease in quality under antitrust law. This marks a significant precedent, illustrating active regulatory intervention at the intersection of data protection and competition. Against this backdrop, the Parliamentary Standing Committee on Finance presented the 53rd Report titled 'Anti-Competitive Practices by Big Tech Companies'[28] to the Lok Sabha on December 22, 2022 (Standing Committee Report). Drawing heavily on the EU's DMA, the Standing Committee Report established a parallel by introducing a similar model, namely the concept of

[24] Report of Competition Law Review Committee, July, 2019.
[25] Market Study on the Telecom Sector in India, Competition Commission of India, 2021.
[26] Shri Vinod Kumar Gupta, Chartered Accountant v. WhatsApp Inc., Case No. 99 of 2016, Competition Commission of India.
[27] WhatsApp LLC v. Competition Commission of India, 2022 SCC OnLine Del 2582.
[28] Report on Anti-Competitive Practices by Big Tech Companies, Standing Committee on Finance, Ministry of Corporate Affairs (Lok Sabha), 2022.

gatekeepers, under the guise of Systemically Significant Digital Enterprises (**"SSDEs"**). Essentially, a select few digital enterprises meeting specific criteria such as revenue, business activity, user base, etc., would be designated as SSDEs, subject to regulatory conditions. On February 6, 2023, the establishment of the Committee on Digital Competition Law (**"CDLC"**) aimed to enact the recommendations put forth by the Standing Committee and in 2024, the CDLC published a draft bill (report) necessitating a separate digital competition law.[29] The CDLC noted that conventional competition jurisprudence has typically leaned towards ex-post intervention models over ex-ante ones due to the risk of false positives, leading to potential over-regulation and a subsequent dampening effect on innovation. However, CDLC highlighted the necessity for reassessment of this premise in the context of Indian digital markets. According to the report, the rapid digitalization of markets significantly impacts the market by demonstrating the strong network effects of large digital enterprises, often resulting in a "winner-takes-all" scenario. The Committee emphasized the necessity of adopting a comprehensive ex-ante model of competition law to address the challenges of modern digital markets. A key recommendation in the DCB aimed at balancing certainty and flexibility. It also outlines essential terminologies related to the nature of services/products and the enterprises covered, while also providing measures for implementing legal recourse.

During the drafting of the DCB, the CDLC considered the possibility of overlap between the DCB and the DPDPA. It concluded that while the DPDPA focuses on safeguarding personal data of data principals, the Competition Act aims to uphold fairness and competitiveness in the market. Therefore, the objectives of both statutes are distinct yet complementary, with no inherent conflict between them. The rapid expansion and increasing significance of data in digital markets have blurred the lines between data protection and competition law. Big Techs distinguish themselves through their access to extensive user data, leveraging it to enhance their products and services. This creates obstacles for new entrants in digital markets that lack access to such vast data reservoirs, consequently diminishing market competitiveness. Moreover, the collection of personal data by these major big techs raises concerns about consumer profiling and the potential sale of data to advertisers for tailoring targeted online offerings, exacerbating worries regarding data privacy.

The CDLC has examined antitrust regulations in other countries, highlighting the focus on ex-ante regulatory models and their necessity for enforcement in Indian digital markets. With the

[29] Digital Competition Bill (Report of the Committee on Digital Competition Law), Ministry of Corporate Affairs, 2024.

rise of large digital enterprises, implementing ex-ante regulations has become crucial for both businesses and consumers. Other nations have already begun adopting ex-ante frameworks, with some successfully enforcing them, such as, the EU had implemented an 'ex-ante framework' through the DMA Regulation in 2022. However, India appears to have taken a softer and liberal stance than the EU's DMA by providing certain exemptions in specific areas such as impact on economic viability, prevention of fraud, cybersecurity threat, prevention of unlawful infringement of IP rights, and other such factors. Similarly, if a company can demonstrate that compliance with the law would result in economic losses, it is not obligated to adhere to the law. Although the draft bill specifies that the CCI will create case-specific exemptions, the general categories for exemptions from ex-ante obligations will be legally established. Unlike the current Competition Act[30], which is ex-post, the DCB mandates that big techs notify the CCI if they qualify as SSDEs. The draft bill broadly prohibits tech companies from engaging in anti-competitive practices, such as restricting third-party apps, self-preferencing, misusing business and end-user data, and bundling products and services. Major big-tech players in the Indian Market like Apple, Google, Amazon, Meta, Uber, and Flipkart have opposed the draft bill, arguing that there are no successful global examples of ex-ante regulations.

Conclusion

Internet (Digital) Platforms now mediate a significant and increasing portion of our commerce and communications. The case studies of Amazon and Meta Platforms in the paper highlight the potential for synergies between data privacy and competition law. However, this also tasks competition and data protection authorities with the challenge of coordinating their respective legal interpretations moving forward. Examining the frameworks in the US through the FTC and in the EU via GDPR and DMA represents a step toward implementing effective measures to address anti-competitive practices and abuses of dominant positions in the digital market sector. However, at this point in India's economic trajectory, adopting a new Digital Competition law modelled after the untested DMA legislation to regulate digital economy players on an ex-ante basis may not produce the desired outcomes. Moreover, India is the birthplace of numerous successful homegrown companies, such as Ola and Oyo so, adopting a DMA-like approach, which essentially promotes a "make not invest" philosophy, could hinder the growth of future success stories. Additionally, the CCI already possesses a robust set of

[30] Competition Act, Acts of Parliament, 2002 (India).

tools, as evidenced by its effective investigations across the digital sector, where many players have faced penalties and also has utilized interim measures in cases like MMT-Oyo to provide swift relief during ongoing investigations, showcasing a viable alternative to ex-ante regulation in digital markets.[31] The proposed DCB derived partly from the Standing Committee Report on Anticompetitive Practices of Big Tech has hindered Indian companies to achieve their requisite economies of scale thus, downgrading their efficiencies. Therefore, instead of promoting a winner-takes-all scenario, this risks causing losses for everyone involved, thus affirming the 'bane' that India is not ready for a Digital Competition Law.

[31]FINANCIAL EXPRESS, https://www-financialexpress-com.cdn.ampproject.org/c/s/www.financialexpress.com/opinion/dont-fix-it-if-its-not-broken/3420558/lite/ (last visited May 2, 2024).