Page 805 - 812 **DOI:** *https://doij.org/10.10000/IJLMH.111372*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 4

2021

Anti-Trust and Privacy: Is It Feasible for Two Laws To Intersect?

SHWETHA. P[1] AND PAVAN KUMAR.R[2]

ABSTRACT

Data privacy, like efficiency, is portrayed in antitrust theory as a factor that increases with competition. The distinctions between antitrust and privacy aims, and enforcement are getting increasingly blurred. The more complicated truth is that, during the previous twenty-five years, data privacy has likewise evolved into its own area of legal theory. In this role, data privacy legislation may collide with antitrust law on the edges, just way intellectual property or consumer protection law did before it. This possibility for antitrust and data privacy to pursue competing goals is especially visible in the digital economy. Consumer data is certainly important in digital competitiveness from an antitrust standpoint. This Article emphasise a novel method to analysing claims involving competing data privacy and competitiveness concerns, emphasising the accommodation of both areas of law.

Keywords: *Data Privacy, Antitrust Law, Separatist, Integrationist, Anticompetative Behaviour.*

I. INTRODUCTION

Antitrust law and data privacy law are important influences affecting how digital information is treated. Both are focusing on the businesses that store and utilise our data, such as Facebook, Google, Apple, and Amazon.[3] These organisations are recurrent favourites of the Federal Trade Commission (FTC) in terms of data privacy enforcement,[4] as well as the stringent new European data protection framework.[5] In a classic antitrust action or merger challenge, the plaintiff would generally present proof that the behaviour at question is likely to result in market or monopolistic power, manifested as higher prices and reduced output. The theory is

[1] Author is an Assistant Professor at B.M.S College of Law, India.
[2] Author is an Associate at White Lion Legal, India.
[3] The term "digital platform" is used here to mean large technology companies whose major services create value by intermediating between different online groups. See, e.g., Ohio v. Am. Express Co., 138 S. Ct. 2274, 2280.
[4] Section 5 of the FTC Act empowers the FTC to prevent unfair or deceptive acts or practices, and that power forms the basis for U.S. data privacy protection outside of sector-specific privacy laws.
[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons about the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1

 [ISSN 2581-5369]

simple: if data is the price that we paying to use these sites will result in market power manifesting itself through reduced levels of privacy.

Although the analogy has numerous flaws, we highlight what we think to be the most significant. First, in what has become known as the "privacy paradox,"[6] empirical data shows that, while consumers pretend to care profoundly about privacy, they do not likely to modify their purchasing decisions based on privacy concerns.[7] The fundamental reason of the privacy paradox is irrelevant: if customers do not respond to businesses' privacy decisions, privacy cannot be an essential component of competition. Second, it is critical to understand that customer data is an input into a broader production process that generates consumer value through more customization and more relevant content (including advertisements).[8] Because privacy costs and data benefits are inversely proportional, and because demand for privacy and a platform's product are heterogeneous and potentially correlated in complex ways, unlike in the case of price, there is not always a negative relationship between data collection and user demand or consumer welfare.[9] We shall now examine the new concept of Intersection of law through the theories of antitrust and privacy.

II. THE ROLE OF DATA IN THE CREATION OF PLATFORM VALUE

Online digital platforms are enterprises that utilise technology to collect content and services and link people for the purposes of interacting, trading, or exchanging information.[10] In a wide range of markets, digital platforms have significantly lowered transaction costs. They have lowered search costs, information prices, and service delivery costs when compared to their offline equivalents by establishing efficiencies that are often unique to platform design and technology.[11] Platforms that are well-designed enable immediate, large-scale connection amongst users, giving a plethora of prospective counterparties for transacting or sharing information inside the same environment. Questions concerning uneven access to relevant data emerge in the situation of digital platforms that provide both a service and act as online

[6] Alex Marthews & Catherine Tucker, Privacy Policy and Competition, ECON. STUD. BROOKINGS 7 (Dec. 2019)

[7] Alastair R. Beresford, Dorothea Kübler, & Sören Preibusch, Unwillingness to Pay for Privacy: A Field Experiment, 17 ECONOMICS LETTERS 25 (2012)

[8] Marc Bourreau, Alexandre de Streel, & Inge Graef, Big Data and Competition Policy: Market Power, Personalised Pricing and Advertising, CENTRE ON REGULATION IN EUROPE, Feb. 16, 2017, https://cerre.eu/sites/cerre/files/170216_CERRE_CompData_FinalReport.pdf at 37

[9] Michael L. Katz, Multisided Platforms, Big Data, and a Little Antitrust Policy, 54 REV. INDUS. ORG. 695 (2019).

[10] We use the term "users" to refer to any sort of user who participates in platform activities. Person end-users as well as individual or corporate players on the opposite side of the platform, such as service providers, media content producers, and advertising, might fall under this category.

[11] Avi Goldfarb & Catherine Tucker, Digital Economics (National Bureau of Econ. Research, Working Paper No. 23684, Aug. 2017)

middlemen for rivals, such as retail platforms publishers. However, the requirements for an antitrust violation are likely to be high, requiring proof that the intermediary service is necessary, and that the discrimination has a significant effect on the market.

III. COMPETITION, PRIVACY, AND CUSTOMER PROTECTION

The European Commission also stated that privacy was a factor in the clearance decisions for Facebook/WhatsApp and Microsoft/LinkedIn.[12] The assessment of any potential negative impact of a merger on privacy is comparable to the standard examination of merger pricing effects. It focuses on the study of the service provider's motives and capacity to erode its consumers' privacy. In the aforementioned merger judgments, privacy deterioration is characterised as the exploitation of newly available user data for targeted commercial purposes. The FTC has been more aggressive in addressing the privacy implications of acquisitions than the European Commission, most likely because it is directly responsible for consumer protection.

IV. EXISTING THEORIES ON THE INTERFACE OF ANTITRUST AND DATA PRIVACY

The convergence of law is a relatively recent phenomenon. The FTC has only created the "new common law of privacy" in the last twenty-five years.[13] From the mid-1990s to the present, the agency's ascension to de facto federal data privacy regulator coincided with the advent of the internet. Individuals were suddenly engaged in a slew of new electronic activities, uploading ever-increasing volumes of data to the internet. Spotty, industry-specific privacy regulations left huge swaths of new internet activity unprotected by data privacy rules.[14] The interaction between antitrust law and data privacy is most innovative in the case of monopoly enforcement.[15] Consider that the development of data privacy regulation corresponds with a twenty-year absence of antitrust prosecution by US antitrust authorities.

Around the time when data privacy legislation began to gain root, "the Sherman Act's anti-monopoly provisions fell into a deep freeze from which they have never really recovered." The initial hypothesis on this legal interface considers data privacy to be outside the scope of antitrust law. This "separatist" viewpoint emphasises the historical and doctrinal separation of the FTC's competition and consumer protection mandates.[16] It promotes the ongoing separation

[12] Comm'n Decision Case M.7217 (Facebook! WhatsApp) 87, 102 (Oc t. 3, 2014).
[13] Daniel J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 COLUM. L. REV. 583, 598-600 (2014).
[14] *ibid*
[15] In merger review, there is a slightly longer history of considering the interaction between antitrust law and data privacy, beginning around 2007 with the FTC's analysis in the Google/Double click merger.
[16] James C. Cooper, Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity, 20 GEO.

of data privacy and antitrust legislation. According to separatist theory, each of these domains of law protects against unique legal evils. Antitrust law is seen to be best adapted to dealing with market behaviour that is damaging to overall consumer welfare or economic efficiency. Given its emphasis on informed choice and reasonable consumer expectations, data privacy regulation is viewed as a better fit for ensuring that individual consumers receive the benefit of their bargains. Separatists are concerned that including privacy issues into antitrust analysis may lead to uncertainty in the application of antitrust law's consumer welfare test.

The second frequently expressed viewpoint on the interaction between antitrust and data privacy contends that antitrust analysis should take data privacy into account if it is a component of quality-based competition. This "integrationist" method includes data privacy into long-established antitrust analysis frameworks.[17] It begins with the well-established stance that competition that is focused not just on price, but also on non-price variables such as quality, improves consumer welfare. It then broadens the definition of "quality" to include privacy-based competition.[18]

Integrationist theory would evaluate the decrease in privacy-as-quality in determining whether the merger will significantly diminish competitiveness. If, on the other hand, there was no privacy-based rivalry between the merging parties, integrationist theory would hold that any privacy issues raised by the merger were outside the scope of antitrust legislation. To date, integrationist theory is the most established and widely accepted perspective on the intersection of antitrust law and data privacy.[19] This integrated perspective has been accepted and utilised in merger cases by the FTC, DOJ,[20] and European competition authorities. Several academics have also endorsed integrationist theory.

Agencies and researchers have tended to stress the complementarity of antitrust and data privacy issues under both separatist and integrationist views. Separatist thought depicts these domains of law as puzzle pieces that are "complementary in nature" but do not overlap. In the same spirit, a merger study that presents data privacy as associated with competitiveness is a common example used to explain integrationist theory. As in the browser example above, integrationist theory analyses whether a transaction is likely to reduce pressure on merging businesses to compete on privacy, resulting in fewer privacy-protective product alternatives for

MASON L. REV. 1129, 1146 (2013)

[17] Erika M. Douglas, Monopolization Remedies and Data Privacy, 24 VA. J.L. & TECH. 2, 25-26 (2020).

[18] National Society of Professional Engineers vs. United States, 435 U.S. 679, 695 (1978)

[19] Geoffrey A. Manne & R. Ben Sperry, The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework, CPI ANTITRUST CHRON., May 2015.

[20] Makan Delrahim, Assistant Attorney Gen., Dep't of Justice, Remarks for the Antitrust New Frontiers Conference: "And Justice for All": Antitrust Enforcement and Digital Gatekeepers (June 11, 2019).

 [ISSN 2581-5369]

customers after the merger. This illustrates a connection in which competitiveness drives privacy, and when one suffers, the other suffers as well. Recent definitions of digital market power and misuse of dominance relate the degradation of data privacy to the decrease of competition.[21]

V. NON-COMPLEMENTARITY EMERGING IN THE DIGITAL ECONOMY

In the digital economy, at least two areas of friction between data privacy and antitrust legislation are emerging. To begin, digital platforms are using data privacy as a commercial reason to defend themselves against charges of anti-competitive behaviour. Second, academics and government organisations are advocating for solutions that provide access to data kept by digital platforms. When such remedies require the disclosure of customers' personal data, they jeopardise data privacy interests. Existing theories do not handle any of these possibilities. They fall into the gap between antitrust and data privacy law interaction as different doctrinal areas of law in a non-complementary manner.

VI. DATA PRIVACY AS A COMMERCIAL JUSTIFICATION FOR ALLEGED ANTI-COMPETITIVE BEHAVIOUR

The Ninth Circuit case HiQ v. LinkedIn case, HiQ's accusations of anti-competitive exclusion are pitted against LinkedIn's rationale for user data privacy protection.[22] HiQ, the complainant, collected information from individual users' LinkedIn social network accounts, which it then utilised to fuel its "people analytics" software.[23] Although LinkedIn first allowed HiQ access to user data, the company eventually banned HiQ from LinkedIn servers. HiQ stated that its company would fail if it did not have access to LinkedIn user data. It said the restriction amounted to unfair competition in support of LinkedIn's own intentions to launch competitive data analytics products.[24]

LinkedIn defended its termination of HIQ'S by citing user privacy interests in LinkedIn profile data. HIQ, it said, was infringing on user data privacy by ignoring user profile preferences. LinkedIn is a popular platform for professional networking. Changes in user profile information may therefore signal an upcoming job search and employment leave.[25] That, in

[21] HOUSE SUBCOMMITTEE REPORT ON COMPETITION IN DIGITAL MARKETS, at 43
[22] hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019). HiQ claimed under California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 et seq. among other causes of action. However, HiQ's argument is very similar to a section 2 Sherman Act refusal-to-deal claim. In fact, the District Court looks to Section 2 of the Sherman Act for guidance on what constitutes an anti-competitive act in state law.
[23] hiQ Labs, 938 F.3d at 991.
[24] *Id. at 998.*
[25] *id*

 [ISSN 2581-5369]

fact, was the concept of HIQ'S software—alerting companies about which of their employees are at risk of quitting their jobs based on changes to the employee's LinkedIn profile. The issue, according to LinkedIn, is that individuals intentionally enabled a privacy setting called "do not broadcast" to prevent such profile updates from being automatically broadcast to their professional social network, including their employers' email boxes.[26] The Ninth Circuit affirmed a preliminary injunction mandating that LinkedIn restore HIQ'S access to customer profile data.[27]

This court scepticism toward user data privacy interests in HIQ v. LinkedIn runs contrary to the FTC's ongoing attempts to safeguard comparable consumer interests in online privacy settings. The FTC has prosecuted Google and Facebook, among other firms, for acquiring data in violation of user data privacy settings or for misleading consumers about their ability to depend on such settings to restrict who sees their information. As part of the new data privacy common law, the FTC requires digital platforms to respect user privacy preferences, such to those ignored by HiQ. LinkedIn might easily have been prosecuted under Section 5 of the FTC Act for deceiving customers regarding their capacity to restrict the publication of their profile information.[28] At least at this early level of relief, this solution favours data-driven competitiveness over data privacy, with little justification as to why this is beneficial for customers.

In reaction to charges of anti-competitive behaviour, other digital platforms are using data privacy as a commercial reason. Google, Apple, and Facebook are all facing separate but related lawsuits or investigations alleging that they banned competitive apps from their internet platforms in violation of antitrust law.[29] Antitrust research has not yet addressed whether the preservation of user data privacy is cognizable as a business rationale. Separatist philosophy does not address this topic since it assumes no connection between these domains of law. Integrationist theory might be used to determine if the claimed protection of data privacy increases customer welfare and so is a possibly legitimate economic justification.[30] However, no court, agency, or academic has yet to address this issue. Regardless, these new situations

[26] An estimated fifty million LinkedIn users chose to engage the “do not broadcast” setting. Once the setting is activated, changes made by the user to their profile are no longer sent via automated e-mail from LinkedIn to the contacts in the user’s LinkedIn social network. When the setting is not engaged, everyone in the users’ network receives an automated alert highlighting the changes in the user’s profile. Id. at 994.
[27] HiQ, 938 F.3d at 1005.
[28] 15 U.S.C. § 45(a)(1) (2018).
[29] H. Comm. on the Judiciary, Subcomm. on Antitrust, Commercial, and Administrative Law, 116th Cong., Investigation of Competition in Digital Markets: Majority Staff Rep. and Recommendations (2020)
[30] Polygram Holding, Inc. v. F.T.C., 416 F.3d 29, 36 (D.C. Cir. 2005) (“Cognizable justifications ordinarily explain how specific restrictions enable the defendants to increase output or improve product quality, service, or innovation.”).

 [ISSN 2581-5369]

clearly do not fit with the prevailing narrative of antitrust/data privacy complementarity. Instead, they juxtapose allegations of anti-competitive behaviour with the claimed commercial reason for customer data privacy protection.

VII. TENSION IN THE HORIZON IN THE UNITED STATES, ACCORDING TO THE EUROPEAN COMPETITION LAW/DATA PROTECTION INTERFACE

The European Union's experience with data privacy and antitrust legislation at the junction foreshadows friction between these two areas of law in the United States. European data protection and competition law duties and enforcement are often more stringent than their American counterparts.[31] This rights-based approach frequently results in better data privacy safeguards than those provided by US law, where the jurisprudential roots are only as deep as consumer protection theory. There is no similar legal duty on monopolist businesses in the United States. European competition regulators have also been far more aggressive than their counterparts in the United States in pursuing abuse of dominance charges against big technological platforms. The European Commission is conducting various investigations into technological behemoths and has already fined Google several times for abuse of power.[32]

VIII. PROPOSAL

The starting point for the analysis should be to give equal weight to both areas of law. This means that neither antitrust nor privacy legislation would be deemed to have precedence over the other in establishing the scope of permissible behaviour. Similarly, action that is promoted or mandated by one area of law is not always immune from the other. Instead, the significance of the various interests at issue in antitrust and data privacy should be examined and measured against one another. In reality, using this approach will necessitate courts and authorities delving into the precise data privacy and competition interests at issue. This would entail considering, on the one hand, the centrality or relevance of the principle being invoked under data privacy legislation, and, on the other, the extent to which the claimed misbehaviour impedes competition. Traditional antitrust analyses of anticompetitive effects and market dominance would continue to be important, but possibly balancing legal issues relating to data privacy would also be considered. Offsetting considerations would be assessed in accordance with data privacy law and the reasonable privacy expectations recognised in it. This suggested analytical paradigm is based on techniques that have evolved throughout time at the

[31] Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391, 397 Art. 8, GDPR
[32] Digital, Culture, Media and Sport Committee, Disinformation and 'Fake News': Final Report, 2017-19, HC 1791, at 38 (UK)

intersections of antitrust and other key areas of law, such as patent and consumer protection.

IX. EPILOGUE

The contemporary condition of antitrust, according to Herbert Hovenkamp, is "caught between its pursuit of technical rules meant to define and execute acceptable economic aims, and more political appeals for a new antitrust 'movement.'"[33] It has become common knowledge that the price we pay for access to online digital services is our privacy. The apparent corollary to this knowledge is that dominant internet platforms exploit their market power by providing less privacy to their customers than they would in a competitive market. Although there is no reason why businesses cannot compete based on the privacy they provide to their customers, the extent to which enterprises would find this dimension of competition appealing is more difficult than it looks at first glance. The relationship between market dominance and privacy is an empirical topic, and our research finds no evidence to support a correlation between market concentration and poorer levels of privacy for Android applications and prominent websites. Where the jurisprudential roots are only as profound as consumer protection theory, as a result, if society feels that digital products provide insufficient privacy, there does not appear to be a competitiveness issue, making antitrust a particularly weak instrument for improving privacy.

*****

[33] Herbert Hovenkamp, Whatever Did Happen to the Antitrust Movement? 94 Notre Dame L. Rev. 583, 583 (2018).

 [ISSN 2581-5369]