STANFORD
COMPUTATIONAL
ANTITRUST

ARTICLE

Computational Presumptions Applied to AI Markets

Alba Ribera Martínez *

Abstract. Digital regulators worldwide are imposing sweeping bans on data combinations to eliminate data asymmetries and learning effects. These interventions reveal a critical disconnect. *Ex ante* regulations ban data combinations across services that fundamentally uproot the functioning of any large language model (LLM). Regulations designed for traditional platforms are now being applied to AI downstream markets, where reinforcement learning, model drift, and nuances between across- and within-user learning create fundamentally different competitive dynamics. As a consequence, *ex ante* regulations risk stifling innovation while failing to address consumer harm. The paper argues for considering computational presumptions that use privacy-preserving techniques as measurable compliance mechanisms. By replacing blunt prohibitions with architectural safeguards grounded in privacy-utility thresholds, regulators can effectively neutralize lock-in effects while preserving the essential data flows for AI advancement and improvement.

KEYWORDS: AI markets; data asymmetries; learning effects; market power; ex ante regulation; computational presumptions; privacy-preserving computation
JEL NOS: K21, L41, D82, O33, K23

* Dr. Alba Ribera Martínez is a Visiting Professor at the Brussels Study Centre. Email: riberamartinezalba@gmail.com. ORCID: 0000-0002-9152-0030. The author joined the Stanford Computational Antitrust as an Editor-in-Chief after submitting the piece for revision, and all reviews of the papers were conducted by a separate panel of editors. The author thanks Thibault Schrepel and Volker Stocker for their comments on a draft version of the paper.

I. Introduction

Digital platforms[1] and ecosystem holders collect and process vast troves of data in their daily business.[2] To cater to the diverse needs of different consumer groups, these digital platforms analyze data to identify patterns and future market demands. Some term such processing and collection of data as unlimited and subject to the logic of surveillance capitalism,[3] whereas others interpret these actions as the cost of doing business.[4]

Different competition authorities and regulators identify two economic characteristics that may lead to market inefficiencies related to the leveraging of data: information asymmetries and learning effects.[5] Learning effects[6] and data asymmetries[7] can both generate externalities when they cause benefits (positive externalities) and/or costs (negative externalities) to third parties.

Asymmetries of information relate to imbalances in the distribution of knowledge. They refute the inherently perfect market of information to demonstrate the convexity of the world.[8] Disparities in control and access to data

---

[1] Digital platforms are normally described as those using digital technology to interact between users and suppliers, see Martin Kenney & John Zysman, *The Rise of the Platform Economy*, 32 ISSUES IN SCI. TECHNOL. 61, 65 (2016).

[2] Federal Trade Commission, *A Look Behind the Screens: Examining the Data Practices of Social media and Video Streaming Services*, FEDERAL TRADE COMMISSION (November 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf.

[3] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 180 (2nd ed. 2019); Alice Marwick, *The Public Domain: Surveillance in Everyday Life*, 9 SURVEILL. SOC. 378, 380 (2012).

[4] David S. Evans, *The Antitrust Economics of Free*, COMPETITION POLICY INTERNATIONAL (May, 17 2011), https://www.competitionpolicyinternational.com/the-antitrust-economics-of-free/.

[5] Bundeskartellamt, *Proceedings against Meta/Facebook* (June 7, 2023), https://www.bundeskartellamt.de/EN/Digital_economy/proceedings_against_large_digital_companies/Meta_Facebook/Meta_Facebook_node.html. Commenting on the case, see Peter J. van de Waerdt, *Meta v Bundeskartellamt: Something Old, Something New*, 8 EUR. PAP. 1077, 1080-1090 (2023); and Anne C Witt, *Meta v Bundeskartellamt – Data-based Conduct Between Antitrust Law and Regulation*, 12 J. ANTITRUST ENFORC. 345, 347 (2024). On asymmetries of information as market failures, Tibor Scitovsky, *The Benefits of Asymmetric Markets*, 4 J. ECON. PERSPECT. 135, 136 (1990).

[6] The author refers to learning effects throughout the paper to account for those arising from the accumulation and use of data. They must not be conflated with human-based network effects, which occur when a product's value increases due to human interaction and the size of the user base.

[7] The author uses the concept of data asymmetries as the translation of information asymmetries taking place in the data parameter of markets. Information and data asymmetries are used as interchangeable notions throughout the paper, to the extent that the author builds on the economic literature surrounding information asymmetries.

[8] Joseph E. Stiglitz, *Information and Economic Analysis: A Perspective*, 95 ECON. J. 21, 22 (1985).

entail that the service provider has access to more information than its users and competitors, because it combines data for personalization and advertising.[9]

Digital platforms acting as data stewards[10] have a greater capacity to unlock more value from that data than any other participant in the market.[11] The situation generates potential positive and negative impacts. On one hand, incumbent digital platforms can take advantage of specialization gains[12] and innovation spillovers[13] when taking their decisions. As a consequence of the aggregation and analysis of large datasets, data stewards can develop innovative or more efficient products and services that benefit consumers. Innovation can subsequently crystallize into knowledge spillovers that other competitors can benefit from.[14] On the other hand, a competitive advantage starts to solidify, which is a byproduct of the market's structure rather than their superior innovation.[15] The competitive advantage that these asymmetries of information report to the data steward comes as a consequence of an inefficient allocation of resources.[16] The data steward gains power not by producing a better product, but rather by capturing data that others cannot access, creating a toll-bridge effect that prevents a level playing field where all players can

[9] Sandra C. Matz & Oded Netzer, *Using Big Data as a Window into Consumers' Psychology*, 18 CURR. OPIN. BEHAV. SCI. 7, 9 (2017).

[10] Data stewards define and enforce the data management policies and procedures within their infrastructures.

[11] Leigh Dodds, *What is data asymmetry?* (24 March 2017), https://blog.ldodds.com/2017/03/24/what-is-data-asymmetry/.

[12] The incumbent platform focuses on its unique knowledge and skills, which fosters its productivity, see David Aboody & Baruch Lev, *Information Asymmetry, R&D, and Insider Gains*, 55 J. FINANC. ECON. 2747, 2750 (2000).

[13] The data steward drives innovation spillovers by creating knowledge gaps where firms learn from peers' R&D, failures and successes. For the relationship between both, see David B. Audretsch & Maksim Belitski, *The knowledge spillover of innovation*, 31 IND. CORP. CHANGE 1329, 1335-1337 (2022); Phuong-Anh Nguyen & Ambrus Kesckés, *Do technology spillovers affect the corporate information environment?* 62 J. CORP. FINANCE 101581, 101594 (2020); and Anne Marie Knott, Hart E. Posen & Brian Wu, *Spillover Asymmetry and Why It Matters*, 55 MANAG. SCI. 373, 382 (2009).

[14] Those can take place either by access to public information available due to patents and licenses being issued or learning by doing, see Oliver Falck & Johannes Koenen, *Resource "Data": Economic Benefits of Data Provision*, 21 CESIFO FORUM 31, 35-37 (2020); and Gregory N. Mandel, *Proxy Signals: Capturing Private Information for Private Information*, 90 WASH. U. L. REV. 1, 17-18 (2012).

[15] This motion likens the chicken-and-egg problem taking place in digital platforms where competing platforms attract initial users (buyers and sellers) when neither side wants to join without the other already present, see Bernard Caillaud & Bruno Jullien, *Chicken & Egg: Competition among Intermediation Service Providers*, 34 RAND J. ECON. 309, 309 (2003).

[16] George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q. J. ECON. 488, 493 (1970); Joseph E. Stiglitz & Andrew Weiss, *Credit Rationing in Markets with Imperfect Information*, 71 AM. ECON. REV. 393, 404 (1981).

compete on the same terms.[17] Such market inefficiencies increase the possibility that consumers engage in adverse selection.[18]

When faced with the choice of disclosing their information upon registration on a digital platform, consumers operate under conditions of structural information asymmetry that preclude any meaningful form of informed consent. The consumer weighs the benefits of personalization (being delivered more relevant ads, reducing information overload, or lower prices[19]) against the potential losses of data disclosure (either the collection of sensitive data or allowing third-party access) to the digital platform.[20] A misallocation of resources happens when the consumer agrees to disclose data even where doing so generates substantially greater value for the platform than any personalization benefit conferred upon the consumer. This dynamic leads to negative outcomes when consumers engage in adverse selection, namely when a consumer selects a low-quality service (the unwanted exchange) because the architecture of digital platforms is structurally designed to prevent its acquisition.[21]

Informationally efficient markets are, in fact, impossible, and digital platforms represent an acute representation of this impossibility.[22] The relevant question is how far structural asymmetries distort their choices beyond what even bounded rationality would predict.

Individual consumers respond to these asymmetries differently, given that the literature already identified systematic heterogeneity across user populations as far as perceptions over potential information disclosures. One cannot, therefore, simply state that the asymmetries of information present in a digital (for free) service amount to streamlined negative externalities. Data asymmetries radically increase

---

[17] Dodds, *supra* note 11.

[18] For information asymmetries, drawing the analogy to data asymmetries, Akerlof, *supra* note 16, at 493; Stiglitz & Weiss, *supra* note 16, at 404; Scitovsky, *supra* note 5, at 136.

[19] Sabrina Karwatzki, Olga Dytynko, Manuel Trenz & Daniel Veit, *Beyond the Personalization-Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization*, 34 J. MANAG. INF. SYST. 369, 370 (2017).

[20] Mary J. Culnan & Pamela K. Armstrong, *Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation*, 10 ORGAN. SCI. 104, 109 (1999); Sophie C. Boerman, Sanne Kruikemeier & Nadine Bol, *When Is Personalized Advertising Crossing Personal Boundaries? How Type of Information, Data Sharing and Personalized Pricing Influence Consumer Perception of Personalized Advertising*, 4 COMPUT. HUM. BEHAV. REP. 100144, 100144 (2021); John T. Gironda & Pradeep K. Korgaonkar, *iSpy? Tailored versus Invasive Ads and Consumers' Perceptions of Personalized Advertising*, 29 ELECTRON. COMMER. RES. APPL. 64, 68 (2018).

[21] Akerlof, *supra* note 16, at 491; and PAUL BELLEFLAMME & MARTIN PEITZ, THE ECONOMICS OF PLATFORMS: CONCEPTS AND STRATEGY 41-76 (1st ed. 2021).

[22] Sanford J. Grossman & Joseph E. Stiglitz, *On the Impossibility of Informationally Efficient Markets*, 70 AM. ECON. REV. 393, 393 (1980).

the incentives of uninformed agents to acquire information, and they will probably turn to data markets crowded by data monopolists and intermediaries.[23]

Learning effects power, the resulting unwanted exchanges initially provoked by data asymmetries.[24] They entail that more data in the hands of a single player means that it will have access to increasing volumes of data about consumers and competitors.[25] The more the service learns from the data it collects on users, the more valuable it becomes for each participant on the platform.[26] User base growth caused by the learning effects is then used to provide recommendations and personalize the service further which, in turn, increases the service's value in a self-reinforcing positive learning loop.[27]

Depending on the type of service, learning effects can be either positively or negatively correlated as well as relatively symmetric or skewed towards the platform holder.[28] On the note of positive correlation, as more users interact with the service, data-driven insights allow the platforms to tailor experiences to individual preferences, which increases user satisfaction and engagement. Continuous data influx enables the platform holder to learn from this data, making the service more accurate and valuable to each user.[29]

---

[23] Grossman & Stiglitz, *supra* note 22, at 401.

[24] W. Brian Arthur characterizes them as positive feedback loops, where early adoption and critical mass dictate winners, often leading to an 'accumulating advantage', see W. Brian Arthur, *Competing Technologies, Increasing Returns, and Lock-in by Historical Events*, 99 ECON. J. 116, 118-119 (1989).

[25] Michael A. Cusumano, *Data Platforms and Network Effects: How Data-Network Effects Create Opportunities and Inflate Expectations*, COMMUNICATIONS OF THE ACM (October 1, 2022), https://cacm.acm.org/opinion/data-platforms-and-network-effects/.

[26] Robert Wayne Gregory, Ola Henfridsson, Evgeny Kaganer & Skolkovo Harris Kyriakou, *The Role of Artificial Intelligence and Data Network Effects for Creating User Value*, 46 ACAD. MANAG. REV. 534, 535 (2021).

[27] Darek M. Haftor, Ricardo Costa Climent & Jenny Eriksson Lundström, *How Machine Learning Activities Data Network Effects in Business Models: Theory Advancement Through An Industrial Case of Promoting Ecological Sustainability*, 131 J. BUS. RES. 196, 198 (2021); Darek M. Haftor, Ricardo Costa-Climent & Samuel Ribeiro Navarrete, *A Pathway to Bypassing Market Entry Barriers from Data Network Effects: A Case Study of a Start-up's Use of Machine Learning*, 168 J. BUS. RES. 1, 4 (2023); AJAY AGRAWAL, JOSHUA GANS & AVI GOLDFARB, PREDICTION MACHINES: THE SIMPLE ECONOMICS OF ARTIFICIAL INTELLIGENCE (1st edition 2022); Shota Ichihashi, *Online Privacy and Information Disclosure by Consumers*, 110 AM. ECON. REV. 569, 572 (2020); Joseph Farrell & Garth Saloner, *Installed Base and Compatibility: Innovation, Product Preannouncements, and Predation*, 76 AM. ECON. REV. 940, 946 (1986); and Michael L. Katz & Carl Shapiro, *Network Externalities, Competition, and Compatibility*, 75 AM. ECON. REV. 424, 428 (1985).

[28] Howard Shelanski, Samantha Knox & Arif Dhilla, *Network Effects and Efficiencies in Multisided Markets*, OECD (November 15, 2017), https://one.oecd.org/document/DAF/COMP/WD(2017)40/FINAL/en/pdf.

[29] Haftor, Costa-Climent & Ribeiro Navarrete, *supra* note 27, at 114240.

Bearing in mind negative correlations, learning effects create path-dependencies due to the cumulative and proprietary nature of the data collected.[30] Data and behavioral insights accumulate over time and permeate into the service's performance. By this same token, positive feedback loops may confer greater competitive advantages to first movers and large players.[31]

Notwithstanding, these service improvements do not happen in a vacuum. A user who switches to a new and superior platform cannot obtain its full benefit unless other users switch and adopt the new platform as a default. Due to the incumbent platform's scale in its prediction capabilities, users who are committed to it will be less prone to adopt a different platform, even if doing so would be socially beneficial for them (excess inertia).[32] They are, therefore, locked into the network. Before changing market conditions and opportunities, consumers do not flow to higher-quality platforms but stay within the suboptimal networked platform. Regulators and competition authorities argue that these dynamics create a cycle leading to market tipping towards a single dominant platform.[33]

To establish whether these negative externalities apply across all digital markets as soon as an economic operator reaches incumbency, one must therefore look at the trajectories of those effects. Foundational work in economics point out that data asymmetries follow the trajectory of a downward spiral, which can be split up into three fundamental phases: resource misallocation, the tipping point, and the network's decline.[34] Once consumers realize resources have been misallocated, they exit the platform. The effect creates a feedback loop that can lead to the platform's collapse. The problem with this formulation is incumbents being entrenched in the

---

[30] David R. Clough & Andy Wu, *Artificial Intelligence, Data-Driven Learning, and the Decentralized Structure of Platform Ecosystems*, 47 ACAD. MANAG. REV. 184, 191 (2022). On top of that, disruptive innovation can always happen outside the boundaries of existing networks, see Clayton M. Christensen, Rory McDonald, Elizabeth J. Altman & Jonathan E. Palmer, *Disruptive Innovation: An Intellectual History and Directors for Future Research*, 55 J. MANAG. STUD. 1043, 1049 (2018).

[31] Farrell & Saloner, *supra* note 27, at 946; and Katz & Shapiro *supra* note 27, at 428.

[32] Farrell & Saloner, *supra* note 27, at 954. That point has been contested by, for instance, S. J. Liebowitz & Stephen E. Margolis, *The Fable of Keys*, 33 J. LAW & ECON. 1, 1 (1990).

[33] Shelanski, Knox & Dhilla, *supra* note 28, at 5; and European Commission, *Impact Assessment Report – Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector*, DIGITAL MARKETS ACT (December 15, 2020), https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-markets-act. Arguing against the simplicity of the theories of network effects, see Raz Agranat & Michal Gal, *The Microsoft Formula for Platform Power: Do Significant Network Effects Inevitably Generate Winner-Takes-All Dynamics?*, SSRN (September 8, 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5424114.

[34] Akerlof, *supra* note 16, at 495; Joseph E. Stiglitz & Andrew Weiss, *Banks as Social Accountants and Screening Devices for the Allocation of Credit*, NBER WORKING PAPER SERIES NO. 2710 (September 1988), https://doi.org/10.3386/w2710.

market.[35] Exiting the platform can be particularly complex for consumers when there are no equivalent alternatives to the incumbent's service.

The trajectory of learning effects is more contested. Most economic models representing learning effects lead to value curves that monotonically increase with network size.[36] Linear increases in user adoption will only apply, however, to those platforms that are sufficiently sticky on the demand side to retain user engagement whilst attracting new users to join the platform. When demand is not sticky enough, the positive externalities from joining a new platform may outweigh the negative ones. By exposing the platform to a negative feedback cycle, consumers may depart from the old platform *en masse*.[37] Increasing returns in a particular network can be tempered by insignificant events, creating path-dependencies that lead to a network's fall, given that they rely on the features of non-predictability and potential inefficiencies.[38]

In parallel, those same models point to the fact that continuous increments in utility cannot hold beyond a limited value.[39] Empirical evidence has shown that diminishing returns to scale apply to some digital platforms precisely because of their difference in terms of structure, distribution, and types of conduct originating in them.[40] Some platforms can get saturated when too many users join them, or the

---

[35] Joan Rodon Modol & Ben Eaton, *Digital Infrastructure Evolution as Generative Entrenchment: The Formation of a Core-Periphery Structure*, 36 J. INF. TECHNOL. 342, 348-355 (2021).

[36] This is the case, for example, for a number of economic models, including Bob Metcalfe, *Metcalfe's Law after 40 Years of Ethernet*, 46 COMPUTER 26, 26 (2013); David P. Reed, *The Law of the Pack*, HARVARD BUSINESS REVIEW (February 2001), https://hbr.org/2001/02/the-law-of-the-pack; and Bob Briscoe, Andrew Odlyzko & Benjamin Tilly, *Metcalfe's Law is Wrong*, 7 IEEE SPECTR. 26, 28 (2006).

[37] Christopher S. Yoo, *Network Effects in Action*,5 THE GLOBAL ANTITRUST INSTITUTE REPORT ON THE DIGITAL ECONOMY 159, 173-174 (2020); David S. Evans & Richard Schmalensee, *Network Effects: March to the Evidence, Not to the Slogans*, COMPETITION POLICY INTERNATIONAL (September 7, 2017), https://www.pymnts.com/cpi-posts/network-effects-march-to-the-evidence-not-to-the-slogans/; and Catherine Tucker, *Why Network Effects Matter Less Than They Used To*, HARVARD BUSINESS REVIEW (June 22, 2018), https://hbr.org/2018/06/why-network-effects-matter-less-than-they-used-to.

[38] Arthur, *supra* note 24, at 161.

[39] Metcalfe *supra* note 36, at 53; and Andrew McAfee & François-Xavier Oliveau, *Confronting the Limits of Networks*, MIT SLOAN MANAGEMENT REVIEW (July 15, 2002), https://sloanreview.mit.edu/article/confronting-the-limits-of-networks/.

[40] Patrick Bajari, Victor Chernozhukov, Ali Hortaçsu & Junichi Suzuki, *The Impact of Big Data on Firm Performance: An Empirical Investigation*, 109 AEA PAPERS AND PROCEEDINGS 33, 34 (2019); Di He, Aadharsh Kannan, Tie-Yan Liu, R. Preston McAfee, Tao Qin & Justin M. Rao, *Scale Effects in Web Search* in WEB AND INTERNET ECONOMICS (Nikhil R. Devanur & Pinyan Lu eds., 2017); Hema Yoganarasimhan, *Search Personalization Using Machine Learning*, 66 MANAG. SCI. 1045, 1052 (2020); Jörg Claussen, Christian Peukert & Ananya Sen, *The Editor vs. the Algorithm: Returns to Data and Externalities in Online News*, CESIFO WORKING PAPER SERIES 8012 (2019), https://doi.org/10.2139/ssrn.3479854.

search costs become unmanageable. Clusters of users may assign substantial value to a part of the platform's services, but not to the overall service.[41] They will be easier to displace in these sets of cases by new entrants, and competition will be more intense for preserving these strategic users.[42]

Regardless of the economic discrepancies that influence data asymmetries and learning effects, regulators consider their compounding effect. When one considers them in a cluster, economic evidence points out that the extent and context in which excess inertia is exhibited may counteract or exacerbate adverse selection.[43]

According to the economic literature on learning effects and data asymmetries, regulators frame both economic characteristics as the main source of power imbalances and market failures taking place in the digital space. Given that they reinforce each other and hinder free and undistorted competition in digital platforms, regulators term them as static and reversible barriers to entry and expansion. The general understanding is that competitors without access to the same vast datasets face significant challenges in entering the market or expanding their operations. The barrier is static because it is based on exclusive ownership of data. Learning effects in favor of incumbent digital firms can go far enough to tip a platform market toward monopoly.[44]

Under this representation, when both economic characteristics are clustered together in their analysis by regulators, they always result in generating winner-takes-all/most market dynamics.[45] These outcomes create oligopolies that stifle competition, leading to market failures by misallocating resources and fostering

---

[41] McAfee & Oliveau, *supra* note 39; JEFFREY H. ROHLFS, BANDWAGON EFFECTS IN HIGH TECHNOLOGY INDUSTRIES 29 (1st ed. 2003).

[42] Feng Zhu, Xinxin Li, Ehsan Valavi & Marco Iansiti, *Network Interconnectivity and Entry into Platform Markets*, HARVARD BUSINESS SCHOOL WORKING PAPER 19-062 (2019), https://www.hbs.edu/ris/Publication%20Files/19-062_ca94ef8a-6589-4210-a598-90900bd772e5.pdf; David S. Evans & Richard Schmalensee, *Debunking the 'Network Effects' Bogeyman*, 36 REGULATION 36, 38 (2018); Bruno Jullien & Wilfried Sand-Zantman, *Network Effects*, RAPPORT IDEI n. 27 (June 2016), https://www.tse-fr.eu/sites/default/files/IDEI/documents/conf/trading2016/rapport/network_effect.pdf.

[43] Documenting the counteracting of adverse selection via excess inertia, see Ramsis R. Croes, Frederik T. Schut & Marco Varkevisser, *Adverse Selection and Consumer Inertia: Empirical Evidence from the Dutch Health Insurance Market*, 26 EUR. J. HEALTH. ECON. 641, 650 (2024). The contrary view can be found, for instance, in Evan Saltzman, Ashley Swanson & Daniel Polsky, Inertia, *Market Power, and Adverse Selection in Health Insurance: Evidence from the ACA Exchanges*, REV. ECON. STAT. 1, 43 (2025).

[44] Shelanski, Knox & Dhilla, *supra* note 28. As a matter of fact, the European regulator explicitly signaled that network effects act as a pre-condition to a market's tipping (a market's gravitation towards a situation of dominance or (quasi-) monopoly, see European Commission, *supra* note 33, at 21. To the contrary, see Agranat & Gal, *supra* note 33.

[45] OECD, EX ANTE REGULATION OF DIGITAL MARKETS (2021).

inefficient excess entry because of high variance in outcomes.[46] The existence of both characteristics elicits regulatory intervention in several jurisdictions, by imposing restrictions, limitations, and outright bans on the processing of data and on data combinations across an undertaking's line of services.[47] This is the particular case for the European Union's Digital Markets Act or the United Kingdom's Digital Markets, Competition and Consumers Act,[48] which have introduced regulatory remedies to eliminate the impacts caused by learning effects and data asymmetries.

A clear question arises from such regulatory intervention. Are both economic characteristics inextricably linked to the emergence of digital markets? The paper takes the example of AI downstream markets[49] as a case study to respond to the question. The newly emergent market differs from traditional digital markets characterized by the presence of digital platforms.[50] The transition from digital platforms to AI downstream markets reveals that without structural intervention, the self-reinforcing positive learning loop can consolidate power, which leads to market tipping and the perpetuation of unwanted exchanges for consumers.

The persistence of learning effects and data asymmetries in this context generates market failures that cannot be self-corrected, making regulatory enforcement necessary. The efficacy of such enforcement hinges on the ability of regulators to match the technological sophistication of the entities they oversee.[51] The paper addresses the challenge by presenting an alternative that competition authorities have already applied in their enforcement: the use of computational

---

[46] Patrick Barwise & Leo Watkins, 1. *The Evolution of Digital Dominance: How and Why We Got to GAFA* in DIGITAL DOMINANCE (Martin Moore & Damian Tambini eds., 2018). In the particular case of data asymmetries, regulators pair the economic characteristic with long-term societal losses in the form of less product variety and less dynamic innovation, see European Commission, *supra* note 33, at 18. For the theory of Big Tech oligopolies, see NICOLAS PETIT, BIG TECH AND THE DIGITAL ECONOMY: THE MOLIGOPOLY SCENARIO (1st ed. 2020).

[47] For example, the European DMA, Regulation 2022/1925, Article 5(2), 2022 O.J. (L 265) 1 (DMA herein) or the Japanese Mobile Software Competition Act, Law No. 58 of 2020, Article 5, 2020 (MSCA herein).

[48] DMA, *supra* note 47; Digital Markets, Competition and Consumers Act 2024, UK Public General Acts, 2024 c. 13 (DMCCA herein)

[49] The paper uses the case study of AI downstream markets, as those which face consumers as a consequence of the development, deployment and provision of AI, notably generative AI.

[50] STUART J. RUSSEL AND PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH (1st ed. 1995); Uthayasankar Sivarajah, Muhammad Mustafa Kamal, Zahir Irani & Vishanth Weerakkody, *Critical Analysis of Big Data Challenges and Analytical Methods*, 70 J. BUS. RES. 263, 270 (2017).

[51] A broader question is yet pending on whether regulators can realistically match the technological sophistication, see William Lehr & Volker Stocker, *Competition Policy over the Generative AI Waterfall* in ARTIFICIAL INTELLIGENCE & COMPETITION POLICY (Alden Abbott & Thibault Schrepel eds., 2024).

techniques.[52] Recent reports signal trends at national competition authorities using computational tools for data collection, analysis, and prediction of anti-competitive behaviors.[53]

The paper, however, applies these computational techniques as a potential regulatory means to temper the negative impacts of learning effects and data asymmetries.[54] By using these tools as a regulatory presumption, authorities can move beyond reactive enforcement and toward a proactive stance that actively tempers the impacts of data monopolization.

To outline its contribution, this paper first examines the impacts of learning effects and data asymmetries in AI markets (Section II). It then evaluates the nature of the current regulatory frameworks, specifically the EU's DMA and the UK's DMCCA, demonstrating how existing regulatory instruments fail to effectively mitigate these market failures (Section III). The paper proposes integrating computational techniques into the regulatory process. This approach establishes safe-harbor requirements that allow regulatory targets to achieve compliance through standardized technical benchmarks (Section IV). Finally, the paper maps out the implementation challenges that this solution would pose and how those would be countered through a sound monitoring infrastructure to ensure a robust enforcement of the current regulatory prohibitions (Section V).

II. Data Asymmetries and Learning Effects

Data asymmetries and learning effects are related economic phenomena applying to digital platforms. Both characteristics rely on the interdependencies between network participants, be that in the context of a search engine, a messaging service, or a social network. Their existence depends on different causes. Data

---

[52] Computational techniques are mathematical models used to numerically study the behaviour of complex systems by means of a computer simulation. Definition extracted from *Computational methods articles from across Nature Portfolio*, https://www.nature.com/subjects/computational-methods. See the recent reports of national competition authorities using computational tools to facilitate their enforcement, Thibault Schrepel & Teodora Groza, *Computational Antitrust Worldwide: Fourth Cross-Agency Report*, SSRN (June 23, 2025), https://dx.doi.org/10.2139/ssrn.5305055; and Thibault Schrepel & Teodora Groza, *Computational Antitrust Within Agencies: 3rd Annual Report*, 4 STAN. COMPUT. ANTITRUST 53, 53 (2024).

[53] Computational antitrust is a new domain of legal informatics seeking to develop computational methods for the automation of antitrust procedures and improvement of antitrust analysis, see Thibault Schrepel, Computational Antitrust: *An Introduction and Research Agenda*, 1 STAN. COMPUT. ANTITRUST 1, 1 (2021).

[54] Some of those techniques draw from Hao Du, Shang Liu, Lele Zheng, Yang Cao, Atsuyoshi Nakamura & Lei Chen, *Privacy in Fine-Tuning Large Language Models: Attacks, Defenses, and Future Directions*, ARXIV (April 6, 2025), https://doi.org/10.48550/arXiv.2412.16504.

asymmetries appear before substantial disparities relating to control and data access to a given network.[55] Learning effects hinge on the aggregated knowledge that an incumbent operator obtains via consumer interactions.[56] Asymmetries and learning effects can reinforce each other within digital platforms. A platform can leverage strong learning effects to maintain its dominant position and control information flows within its ecosystem to its own advantage.[57] In turn, high participation in a network can increase the quality of information available to every one of the participants, allowing users to make better decisions.[58]

The general understanding is that, if left unchecked, data asymmetries can steer consumers towards adverse selection and result in socially inefficient outcomes.[59] Due to this reason, the diagnosis performed by competition authorities and regulators is one and the same for both economic outcomes. Regulators assume away their nuances in favor of imposing *ex ante* obligations to counter barriers to entry and expansion. Economic evidence and research provide a much more complex picture relating to the externalities they generate,[60] the trajectories they normally exhibit, and the sources of economic power that precipitate them.

Enter AI with the waves it has sent across competition policy. The explosion in the popularity of chatbots[61] makes the challenge of capturing digital dynamics

---

[55] Stefaan G. Verhulst, *The Ethical Imperative to Identify and Address Data and Intelligence Asymmetries*, 39 AI SOC. 411, 412 (2024).

[56] Some authors also refer to these learning effects as data-enabled learning, see Andrei Hagiu & Julian Wright, *Data-enabled Learning, Network Effects, and Competitive Advantage*, 54 RAND J. ECON. 638, 654-655 (2023).

[57] Fujun Lai, Jian Wang, Chang-Tseh Hsieh & Jeng-Chung (Victor) Chen, *On Network Externalities, E-Business Adoption and Information Asymmetry*, 107 IND. MANAG. DATA SYST. 728, 732 (2007); and Amir Sasson & Øystein Fjeldstad, *Information-Mediated Network Effects: Network Composition and Customer Benefit in the Presence of Information Asymmetry*, 7 STRATEG. ORGAN. 355, 363 (2009).

[58] This argument has been explored in the banking sector, see Sasson & Fjeldstad, *supra* note 57, at 370.

[59] OECD, *supra* note 45; CMA, IMPACT ASSESSMENT – A NEW PRO-COMPETITION REGIME FOR DIGITAL MARKETS (2023); Sean F. Ennis, *Independent Sector Regulators and their Relationship with Competition Authorities*, OECD (December 2, 2019), https://one.oecd.org/document/DAF/COMP/WP2(2019)3/en/pdf; European Commission, *supra* note 33.

[60] Digital platforms also manage these externalities as a core business capability, see Michael G. Jacobides, Carmelo Cennamo & Annabelle Gawer, *Externalities and complementarities in platforms and ecosystems: From structural solutions to endogenous failures*, 53 RES. POLICY 104906, 104907-104910 (2024); and Bruno Jullien & Wilfried Sand-Zantman, *The Economics of Platforms: A Theory Guide for Competition Policy*, 54 INF. ECON. POLICY 100880, 100885 (2021).

[61] Chatbots have become widely popularized in the last years and impacted consumer behavior and attitudes since then, see Kanishka Pathak, Gyan Prakash, Ashutosh Samadhiya, Anil Kumar & Sunil Luthra, *Impact of Gen-AI chatbots on consumer services experiences and behaviors:*

through static regulatory approaches more salient. The underlying concerns around information asymmetries and learning effects meet again as the touchstones where those two worlds collide.

Learning effects characterize AI downstream markets because they drive and entrench the competitive dynamics taking place in them.[62] As AI models process larger volumes of data, their predictive accuracy and output quality improve, by attracting more users that generate more interaction data, and reinforcing the model's advantages in a self-reinforcing feedback loop. These learning effects create barriers to entry, since rivals lacking equivalent data volumes cannot replicate incumbent performance, regardless of their underlying architectural choices. Without data, AI models and systems would have no reason to exist, since they are the lifeblood of their functioning. AI providers[63] train their models on vast amounts of text and data scraped from the Internet, as well as on smaller datasets containing carefully crafted examples of inputs and desired outputs.[64]

Aside from obtaining data from scraping, data acquisition operates through three principal channels that are unequally accessible across the market. First, operators with market power control proprietary datasets that provide them with unique insights to the exclusion of their competitors.[65] Second, they engage in preferential partnerships with high-quality data providers, generating evident data disparities.[66] Third, these combined advantages generate compounding data

---

Focusing on the sensation of awe and usage intentions through a cybernetic lens, 82 J. RETAIL. CONSUM. SERV. 104120, 104120 (2025).

[62] Agrawal, Gans & Goldfarb, *supra* note 27, at 32; Michal S. Gal & Daniel L. Rubinfeld, *Algorithms, AI, and Mergers*, 85 ANTITRUST L. J. 683, 690-691 (2024). This need is particularly salient for generative AI, see Philippe Lorenz, Karine Perset & Jamie Berryhill, Initial Policy *Considerations for Generative Artificial Intelligence*, OECD ARTIFICIAL INTELLIGENCE PAPERS NO. 1 (September 2023), https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/09/initial-policy-considerations-for-generative-artificial-intelligence_1a9ab450/fae2d1e6-en.pdf.

[63] The paper references AI providers as those developing and placing AI systems or general-purpose AI models on the market, mirroring the EU's AI Act definition, see Regulation 2024/1689, 2024 O.J. (L 1689) 1.

[64] Charlotte A. Tschider, *AI's Legitimate Interest: Towards a Public Benefit Privacy Model*, 21 HOUS. J. HEALTH L. & POLICY 125, 132 (2021); Tanner Kohler, *How AI Models Are Trained*, NN/G (May 2, 2025), https://www.nngroup.com/articles/ai-model-training/.

[65] Richard May, *Artificial Intelligence, Data and Competition*, OECD (May 6, 2024), https://one.oecd.org/document/DAF/COMP(2024)2/en/pdf.

[66] Stefan Hunt, Wen Jian, Aman Mawar & Bartley Tablante, *You Are What You Eat: Nurturing Data Markets to Sustain Healthy Generative AI Innovation*, COMPETITION POLICY INTERNATIONAL (November 14, 2023), https://cdn.prod.website-files.com/66cc68fc984f55062a489fe2/66fd5a1985d19eeeaea7d440_you-are-what-you-eat.pdf; and COMPETITION AND MARKETS AUTHORITY, AI FOUNDATION MODELS: UPDATE PAPER (2024).

disparities that further consolidate the position of established providers relative to new entrants.

AI providers further learning by guiding the model when it delivers its results and by re-training it on this data (reinforcement learning from human feedback or RLHF).[67] Reinforcement learning is a computational approach to understanding and automating goal-directed learning and decision-making.[68] An economic agent learns (and applies those results to its outputs) through dynamic interactions with the environment.[69] For example, it leads to the production of more natural-sounding text and of plausible conversational responses in chatbot-like settings.[70]

The value of data collected on real-world human interactions is essential to all these tasks, since AI models trained on recursively generated data tend to collapse.[71] According to neural scaling laws, increasing the size of the training dataset is essential for improving its performance, to ensure comprehensive model coverage and minimize overfitting.[72] Some studies suggest that high quality data reduces the

---

[67] Majid Ghasemi & Dariush Ebrahimi, *Introduction to Reinforcement Learning*, ARXIV (December 2024), https://doi.org/10.48550/arXiv.2408.07712; and Sheen S. Levine & Dinkar Jain, *How Network Effects Make AI Smarter*, HARVARD BUSINESS REVIEW (March 14, 2023), https://hbr.org/2023/03/how-network-effects-make-ai-smarter. Reinforcement learning from human feedback has become the dominant approach for aligning LLMs with human preferences, see Subramanyam Sahoo, Aman Chadha, Vinija Jain & Divya Chaudhary, *Position: The Complexity of Perfect AI Alignment – Formalizing the RLHF Trilemma*, ARXIV (November 23, 2025), https://doi.org/10.48550/arXiv.2511.19504. Despite RLHF is predominant, other types of learning are illustrated on the paper.

[68] RICHARD S. SUTTON & ANDREW G. BARTO, REINFORCEMENT LEARNING: AN INTRODUCTION 15 (1st ed. 2015).

[69] Weihao Tan, Wentao Zhang, Shanqi Liu, Longtao Zheng, Xinrun Wang & Bo An, *True Knowledge Comes from Practice: Aligning LLMs with Embodied Environments via Reinforcement Learning*, ARXIV (March 11, 2024), https://doi.org/10.48550/arXiv.2401.14151.

[70] Adam Dahlgren Lindström, Leila Methnani, Lea Krause, Petter Ericson, Íñigo Martínez de Rituerto de Troya, Dimitri Coelho Mollo & Roel Dobbe, *Helpful, Harmless, Honest? Sociotechnical Limits of AI Alignment and Safety through Reinforcement Learning from Human Feedback*, 27 ETHICS INF. TECHNOL. 1, 1 (2025).

[71] Model collapse entails that the generated data pollute the training set, making the AI model misperceive reality, see Ilia Shumailov, Zakhar Shumaylov, Yiren Zhao, Nicolas Papernot, Ross Anderson & Yarin Gal, *AI Models Collapse When Trained on Recursively Generated Data*, 631 NATURE 755, 755 (2024).

[72] Tom Henighan, Jared Kaplan, Mor Katz, Mark Chen, Christopher Hesse, Jacob Jackson, Heewoo Jun, Tom B. Brown, Prafulla Dhariwal, Scott Gray, Chris Hallacy, Benjamin Mann, Alec Radford, Aditya Ramesh, Nick Ryder, Daniel M. Ziegler, John Schulman, Dario Amodei & Sam McCandlish, *Scaling Laws for Autoregressive Generative Modeling*, ARXIV (November 6, 2020), https://doi.org/10.48550/arXiv.2010.14701; Jordan Hoffmann, Sebastian Borgeaud, Arthur Mensch, Elena Buchatskaya, Trevor Cai, Eliza Rutherford, Diego de Las Casas, Lisa Anne Hendricks, Johannes Welbl, Aidan Clark, Tom Hennigan, Eric Noland, Katie Millican, George van den Driessche, Bogdan Damoc, Aurelia Guy, Simon Osindero, Karen Simonyan, Erich Elsen, Oriol Vinyals, Jack W. Rae & Laurent Sifre, *Training Compute-Optimal Large*

need for extensive datasets, lowering training costs and improving model performance.[73] Above a certain threshold, data quantities positively affect the model's accuracy but may degrade performance.[74] Diminishing marginal utilities of data apply to the initial training of AI models.[75] The quality and uniqueness of data stand as the key characteristics to ensure an AI model's competitiveness.[76]

Language Models, NIPS'22: PROCEEDINGS OF THE 36TH INTERNATIONAL CONFERENCE ON NEURAL INFORMATION PROCESSING SYSTEMS 30016, 30016 (2022). Coverage refers to the portion of data that a model successfully predicts or classifies with high confidence or high precision, see Nadav Har-Tuv, *Coverage vs. Accuracy: Striking a Balance in Data Science*, TOWARDS DATA SCIENCE (April 16, 2024), https://towardsdatascience.com/coverage-vs-accuracy-striking-a-balance-in-data-science-d555415eebe4/. Overfitting entails the model accurately represents the training data but fails to generalize to new data sampled from the same distribution because it learns non-representative patterns, see Constantin Aliferis & Gyorgy Simon, Overfitting, *Underfitting and General Model Overconfidence and Under-Performance Pitfalls and Best Practices in Machine Learning and AI*, in ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN HEALTH CARE AND MEDICAL SCIENCES: BEST PRACTICES AND PITFALLS 477-524 (Gyorgy J. Simon & Constantin Aliferis eds., 2024). Fuzhao Xue, Yao Fu, Wanchunshu Zhou, Zangwei Zheng & Yang You, *To Repeat or Not to Repeat: Insights from Scaling LLM under Token-Crisis*, NIPS'23: PROCEEDINGS OF THE 37TH INTERNATIONAL CONFERENCE ON NEURAL INFORMATION PROCESSING SYSTEMS 59304, 59304 (2023); and Hunt, Jian, Mawar & Tablante, *supra* note 66, at 3.

[73] Jean Kaddour, *The MiniPile Challenge for Data-Efficient Language Models*, ARXIV (April 17, 2023), https://doi.org/10.48550/arXiv.2304.08442; Xiaoqi Jiao, Yichun Yin, Lifeng Shang, Xin Jiang, Xiao Chen, Linlin Li, Fang Wang, and Qun Liu, *TinyBERT: Distilling BERT for Natural Language Understanding*, FINDINGS OF THE ASSOCIATION FOR COMPUTATIONAL LINGUISTICS 4163 (2020); and Guillaume Wenzek, Marie-Anne Lachaux, Alexis Conneau, Vishrav Chaudhary, Francisco Guzmán, Armand Joulin & Edouard Grave, *CCNET: Extracting High Quality Monolingual Datasets from Web Crawl Data*, PROCEEDINGS OF THE TWELFTH LANGUAGE RESOURCES AND EVALUATION CONFERENCE 4003, 4003 (2020).

[74] Aryan Sajith & Krishna Chaitanya Rao Kathala, *Is Training Data Quality or Quantity More Impactful to Small Language Model Performance?*, ARXIV (July 15, 2025), https://doi.org/10.48550/arXiv.2411.15821.

[75] Agrawal, Gans & Goldfarb, *supra* note 27, at 44; and Raz Agranat & Michal S. Gal, *Fueling Concentration: AI Agents and Network Effects*, NETWORK LAW REVIEW (May 1, 2025), https://www.networklawreview.org/ai-agents-network-effects/.

[76] Quality of data follows the dimensions of usability, accuracy, relevance and time-dependency as pointed out by Hunt, Jian, Mawar & Tablante, *supra* note 66, at 4, stemming from Marco Iansiti, *The Value of Data and Its Impact on Competition*, HARVARD BUSINESS SCHOOL WORKING PAPER 22-002 (2021), https://www.hbs.edu/ris/Publication%20Files/22-002submitted_835f63fd-d137-494d-bf37-6ba5695c5bd3.pdf. Scaling refers to how the dataset's size improves model performance and costs, see pages 9-10. Hunt, Jian, Mawar & Tablante, *supra* note 66, at 3; and Thibault Schrepel & Alex 'Sandy' Pentland, *Competition Between AI Foundation Models: Dynamics and Policy Recommendations*, IND. CORP. CHANGE 1, 5 (2024). Uniqueness factors exclusivity and imitability as its key characteristics, see ibid., 10-11; as well as Anja Lambrecht & Catherine E. Tucker, *Can Big Data Protect a Firm From Competition?*, COMPETITION POLICY INTERNATIONAL (2017), https://www.competitionpolicyinternational.com/wp-content/uploads/2017/01/CPI-

However, specialized smaller players with small datasets now can compete with larger players due to technological developments.[77] The democratization of Low-Rank Adaptation (LoRA),[78] Retrieval-Augmented Generation (RAG)[79] and efficient transformer architectures[80] allow smaller players to achieve high-performance and specialized models without requiring massive and pre-trained datasets.

Once a company achieves learning effects, that places the AI provider in a position to improve its AI model as a consequence of consumer interactions with it through RLHF, in a self-reinforcing cycle.[81] RLHF has proven effective in aligning a model with human preferences, but gathering high-quality data is expensive, and its pipeline is considerably complex.[82] Due to this reason, other types of scaling are currently being explored, such as reinforcement learning from AI feedback (RLAIF), which trains the model on preferences generated by an off-the-shelf LLM[83] or Direct

---

Lambrecht-Tucker.pdf; and Charles I. Jones & Christopher Tonetti, *Nonrivalry and the Economics of Data*, 110 AM. ECON. REV. 2819, 2824 (2020).

[77] Tom Dotan, *For AI Giants, Smaller is Sometimes Better*, THE WALL STREET JOURNAL (July 6, 2024), https://www.wsj.com/tech/ai/for-ai-giants-smaller-is-sometimes-better-ef07eb98.

[78] LoRA reduces the number of trainable parameters by 10,000 times and the GPU memory requirement by 3 times, while performing on-par or better than fine-tuned models, see Edward J. Hu, Yelong Shen, Phillip Wallis, Zeyuan Allen-Zhu, Yuanzhi Li, Shean Wang, Lu Wang, Weizhu Chen, *LoRA: Low-Rank Adaptation of Large Language Models*, ARXIV (October 16, 2021), https://doi.org/10.48550/arXiv.2106.09685.

[79] RAG utilizes existing open-source or API-based LLMs and enhances them with its own domain-specific and proprietary data, see Agada Joseph Oche, Ademola Glory Folashade, Tirthankar Ghosal & Arpan Biswas, *A Systematic Review of Key Retrieval-Augmented Generation (RAG) Systems: Progress, Gaps, and Future Directions*, ARXIV (July 25, 2025), https://doi.org/10.48550/arXiv.2507.18910.

[80] Transformer architecture was fundamentally altered, for instance, by DeepSeek, by focusing on extreme efficiency for long-context inference, see DeepSeek-AI, *DeepSeek-V2: A Strong, Economical, and Efficient Mixture-of-Experts Language Model*, ARXIV (June 19, 2024), https://doi.org/10.48550/arXiv.2405.04434.

[81] May, *supra* note 65. This motion, however, might be limited, as pointed out by Schrepel & Pentland, *supra* note 76, at 1091.

[82] Rafael Rafailov, Archit Sharma, Eric Mitchell, Stefano Ermon, Christopher D. Manning & Chelsea Finn, *Direct Preference Optimization: Your Language Model is Secretly a Reward Model*, ARXIV (July 29, 2024), https://doi.org/10.48550/arXiv.2305.18290.

[83] Yuntao Bai, Saurav Kadavath, Sandipan Kundu, Amanda Askell, Jackson Kernion, Andy Jones, Anna Chen, Anna Goldie, Azalia Mirhoseini, Cameron McKinnon, Carol Chen, Catherine Olsson, Christopher Olah, Danny Hernandez, Dawn Drain, Deep Ganguli, Dustin Li, Eli Tran-Johnson, Ethan Perez, Jamie Kerr, Jared Mueller, Jeffrey Ladish, Joshua Landau, Kamal Ndousse, Kamile Lukosuite, Liane Lovitt, Michael Sellitto, Nelson Elhage, Nicholas Schiefer, Noemi Mercado, Nova DasSarma, Robert Lasenby, Robin Larson, Sam Ringer, Scott Johnston, Shauna Kravec, Sheer El Showk, Stanislav Fort, Tamera Lanham, Timothy Telleen-Lawton, Tom Conerly, Tom Henighan, Tristan Hume, Samuel R. Bowman, Zac Hatfield-Dodds, Ben Mann, Dario Amodei, Nicholas Joseph, Sam McCandlish, Tom Brown & Jared

Preference Optimization (DPO), which bypasses the complexity of RLHF by using a simple classification loss on preferred and rejected responses stemming from feedback.

Whether learning effects power sizable feedback loops for large players in downstream markets related to AI is a controversial issue. A significant part of training data is non-rivalrous and non-exclusive. Multiple AI providers may draw on overlapping datasets to achieve comparable baseline outcomes.[84] Notwithstanding, this observation does not extend uniformly across all data types because proprietary datasets and data secured through preferential partnerships retain meaningful exclusivity. It is precisely these data categories that drive competitive disparities among providers.

Data disparities may, therefore, cause large and smaller players to access different volumes of data, but the difference might not translate into a pronounced increase in the model's improvement in the former case. Limitations on learning cross-cut state-of-the-art AI models, for instance, when AI systems cannot adapt fast or efficiently enough to consumer responses because feedback signals are weak.[85] Reinforcement learning struggles with exploration-exploitation trade-offs[86] and generalization.[87] This type of learning might over-exploit popular items of feedback, but it can miss niche content, whilst it also lacks adaptability when deployed in environments that vary unpredictably.

Unlike traditional digital platforms, data asymmetries and learning effects in the provision and development of AI models do not conform to the standard economic assumptions underlying learning effects. Conventional platform economics assumes that data accumulation produces proportional improvements in service quality. In turn, this generates self-reinforcing feedback loops that entrench incumbents and systematically harm third parties through data asymmetries. Neither assumption holds uniformly in AI downstream markets. In the particular case of data asymmetries, the relationship between data volume and model improvement is subject to diminishing returns. In other words, data disparities do not translate directly into equivalent performance disparities. In addition, the

---

Kaplan, *Constitutional AI: Harmlessness from AI Feedback*, ARXIV (December 15, 2022), https://doi.org/10.48550/arXiv.2212.08073.

[84] Andrei Hagiu & Julian Wright, *Artificial Intelligence and Competition Policy*, INT. J. IND. ORGAN. 1, 1 (2025).

[85] Hagiu & Wright, *supra* note 84, at 5-6.

[86] Da Wang, Wei Wei, Lin Li, Xin Wang & Jiye Liang, *Rethinking exploration-exploitation trade-off in reinforcement learning via cognitive consistency*, 187 NEURAL NETW. 107342, 107342 (2025).

[87] Yiding Jiang, J. Zico Kolter & Roberta Raileanu, *On the Importance of Exploration for Generalization in Reinforcement Learning*, ARXIV (June 8, 2023), https://doi.org/10.48550/arXiv.2306.05483.

welfare effects of data asymmetries in AI markets are more ambiguous than traditional models predict. Positive externalities may offset the negative impact of data disparities imposed on third parties.[88] Data disparities arise when consumers lack the ability to understand, on one hand, the data types and scopes processed by the model and, on the other hand, the underlying processes responsible for producing automated decisions.[89] Their translation into negative externalities will only follow when the AI model is sufficiently explainable to the provider.

Learning effects compensate incumbents for the degenerative trajectory of data asymmetries, since they manifest in a recursive feedback loop originating from the AI model's interaction with reality. These effects manifest in the form of a data flywheel.[90] The model feeds on user interactions by generating new data, which is in turn used to refine and improve the model. In a self-reinforcing feedback loop, the model attracts more users and produces yet more interaction data. Major AI providers have explicitly built and scaled these flywheel mechanisms by using real-world user interactions as a continuous source of fine-tuning signal alongside their initial training data. The system's output feeds back into its own development, via automated and non-automated means, as a consequence of increasing user interaction. By doing so, it compounds the learning advantages of incumbents over time.

It bears noting that user participation in these flywheels is not unconditional. AI providers offer users the possibility to opt out of having their conversations used for model training.[91] Data sharing is enabled by default and requires an affirmative user action to disable. The impacts of the opt-out are purely prospective, so that the user's action stops future data from entering the training pipeline, but it does not affect previous user interaction.

The extent to which those learning effects crystallize into excess inertia in favor of large players depends on the nature of self-learning produced by the AI

[88] For an example of the application of generative AI to compensate the effects of adverse selection, see Yukun Zhang & Tianyang Zhang, *Generative AI and Information Asymmetry: Impacts on Adverse Selection and Moral Hazard*, ARXIV (February 18, 2025), https://doi.org/10.48550/arXiv.2502.12969.

[89] Verhulst, *supra* note 55, at 413.

[90] Huseyin Gurkan & Francis de Véricourt, *Contracting, Pricing, and Data Collection Under the AI Flywheel Effect*, 68 MANAG. SCI. 8791 (2022); and Yuzhou Chen & Yulin Zhang, *Pricing, Mergers, and Regulation under the AI Flywheel Effect*, 46 MANAG. DECIS. ECON. 4170, 4170 (2025).

[91] For instance, see OpenAI's policy here, OpenAI, *Privacy Policies and Data Controls*, OPENAI (February 6, 2026), https://openai.com/policies/privacy-policy/.

model. Some economic evidence even holds that more capable learning models can deliver non-diminishing and even super-additive returns.[92]

Assuming that most AI providers may access similar data, data-enabled learning can drive two types of feedback loops: across-user learning and within-user learning.[93] Across-user learning corresponds to the notion of learning effects. More users generate more data when they interact with the AI model, which enables the model's overall improvement. Such an improvement yields increments in utility for all users.[94] Within-user learning, however, is less concerned with the impact of learning effects more broadly. More usage by an individual user enables the AI to improve specifically for that user. Utility improvements only happen at the individual level and do not report any value to an additional user.[95]

An AI model's enhanced within-user learning increases the efficiency of across-user learning.[96] Within-user learning tailors the general model to individual patterns, preferences, and behaviors as a pre-processing step by highlighting the importance of distinct user-specific features. The resulting clean and high-quality data signals the unique patterns to overcome heterogeneity via transfer learning, where the insights gained individually accelerate across-user learning. Besides that, the AI model's generalization is enhanced as a result, making it more flexible and capable of handling new and unseen users efficiently.[97]

Firms benefitting from within-user learning exhibit compounding switching costs for existing customers but remain vulnerable to competition for new consumers, whereas those relying on across-user learning will be more likely to experience winner-takes-most dynamics for both new and existing users.[98] AI downstream markets will be prone to favor a single economic agent when they feed on across-user learning, whereas they will be more path-dependent at the individual level when they build on within-user learning.

This conclusion is mainly held for AI providers who develop and deploy closed AI models. That is, for those AI providers who cater their LLMs through a proprietary

---

[92] Gunhaeng Lee & Julian Wright, *Recommender Systems and the Value of User Data*, SSRN (November 1, 2025), https://dx.doi.org/10.2139/ssrn.5690545.

[93] Hagiu & Wright, *supra* note 56, at 654-655.

[94] *Ibid*., at 645.

[95] Hagiu & Wright *supra* note 84, at 7.

[96] Maximilian Schaefer & Geza Sapi, *Complementarities in Learning from Data: Insights from General Search*, 65 INF. ECON. POLICY 101063, 101085 (2023).

[97] Laura Abrardi, Carlo Cambini & Laura Rondi, *Artificial Intelligence, Firms and Consumer Behavior: A Survey*, 36 J. ECON. SURV. 969, 974 (2021); and Schaefer & Sapi, *supra* note 96, at 101075.

[98] Volker Stocker & William Lehr, *The Growing Complexity of Digital Economies over the GenAI Waterfall: Challenges and Policy Implications*, NETWORK LAW REVIEW (May 2025), https://www.networklawreview.org/stocker-lehr-ecosystem/.

and black-box system offering API integration at a higher cost. They create a cumulative, irreversible history of interaction with the user that dictates the future performance of the model for that specific user. Key examples include OpenAI's ChatGPT, Anthropic's Claude, and Google's Gemini. In other words, the main economic players that regulators are already targeting for their rapid ascent in market shares and market power.[99] These models account for nearly 80% of all AI tokens processed on the leading AI inference platform.

On leading AI inference platforms, less expensive open-weights models account for only 20% of AI tokens processed and roughly 4% of revenue, compared to approximately 80% of tokens and over 95% of revenue captured by closed models from large AI providers.[100] Open-weights models ensure that the negatively tainted aspect of within-user learning can be accessed by competitors by enabling direct access to model parameters for local deployment and customization. Users can adopt these models to private or proprietary datasets for personalized applications. Lock-in is not caused in a top-down motion as with closed models, but rather, personalization is achieved when the user supports the creation of a personalized AI agent.

Open-weights models benefit from significantly lower prices than closed models because they enable inference at only the cost of compute power, with no proprietary API markup. Despite a lag in performance in the short term, the pace at which open-weights models are closing the gap with closed counterparts is accelerating.[101] The continued domination of closed models suggests a significant underutilization of open-weights alternatives that cannot be explained by price or performance differentials alone. Instead, switching costs and trust asymmetries erode consumer choice that would operate in favor of open-weights models.[102] The deeper structural explanation for this phenomenon lies in within-user learning and the path dependencies it generates. Closed models accumulate personalized interaction data over time. They progressively build a user-specific understanding of user preferences and their behavioral patterns. Migrating to an open-weights alternative requires users to forfeit this accumulated learning and restart the personalization process from scratch. The depth of personalized learning embedded in closed models sustains their competitive entrenchment. However, it bears

[99] As a matter of fact, the European Commission has recently triggered a sanctioning proceeding under its prohibition of an abuse of a dominant position against Google based on the content it uses to deliver its AI services, see European Commission, *Commission opens investigation into possible anticompetitive conduct by Google in the use of online content for AI purposes*, PRESS CORNER (December 9, 2025), https://ec.europa.eu/commission/presscorner/detail/da/ip_25_2964.

[100] Frank Nagle & Daniel Yue, *The Latent Role of Open Models in the AI Economy*, SSRN (November 18, 2025), https://dx.doi.org/10.2139/ssrn.5767103.

[101] *Ibid*., at 2-3.

[102] *Ibid*., at 3-4.

remarking that the ε-based auditing framework proposed operates on the assumption of centralized data collection and is not directly transposable to open-weights models deployed locally, where no such data flows exist. The computational presumption is therefore scoped to closed-model architectures and centralized AI service providers.

Data inputted into an AI model does not simply stay stagnant and power these learning effects and feedback loops into eternity so that large players can enjoy a quiet life. AI models normally suffer from model drift[103] due to two main reasons. On one side, models built with historical data cannot accurately interpret the current environment and reliably make precise predictions. On the other side, changes in data (data drift[104]) or in the relationships between input and output variables negatively affect the model's performance (concept drift[105]).

Several competition authorities[106] have already identified risks to competition related to an AI provider's grip on data and the capacity of these markets to exert winner-takes-most competitive dynamics.[107] These concerns apply to two analytically distinct categories of economic players. The first encompasses Big Tech incumbents, including Google, Microsoft, Amazon, and Apple, whose competitive advantages in AI derive substantially from proprietary datasets and ecosystem lock-in accumulated through their pre-existing dominance in digital services. The second comprehends AI-native providers, such as OpenAI and Anthropic, whose data advantages are not legacy-derived. They consolidate rapidly through data flywheel effects and first-mover accumulation of interaction data at scale. In both cases, regulators have drawn attention to the fact that key inputs, such as data, controlled by these digital players may lead to high barriers to entry that hinder potential rivals to develop or deploying capable models providing the building blocks for a competitive alternative.[108] These regulators highlight that smaller players cannot gain lasting advantages in the market as a consequence of the small size of their networks. They cannot thrive on those increments in utility, whereas larger players

---

[103] Ricky E. Carter, Vidhu Anand, David M. Harmon Jr. & Patricia A. Pellikka, *Model Drift: When It Can Be A Sign of Success And When It Can be an Occult Problem*, 6 INTELL-BASED MED. 100058, 100058 (2022).

[104] Samuel Ackerman, Orna Raz, Marcel Zalmanovici & Aviad Zlotnick, *Automatically Detecting Data Drift in Machine Learning Classifiers*, ARXIV (November 10, 2021), https://doi.org/10.48550/arXiv.2111.05672.

[105] Fabian Hinder, Valerie Vaquet, Johannes Brinkrold & Barbara Hammer, *Model-Based Explanations of Concept Drift*, 555 NEUROCOMPUTING 126640, 126640-126641 (2023).

[106] Competition and Markets Authority, *supra* note 66; COMPETITION BUREAU CANADA, ARTIFICIAL INTELLIGENCE AND COMPETITION (2024); AUTORIDADE DA CONCORRÊNCIA, COMPETITION AND GENERATIVE ARTIFICIAL INTELLIGENCE (2023).

[107] Competition and Markets Authority, *supra* note 66.

[108] *Ibid*., at 14.

enjoy a lasting advantage due to the relationship between their formerly 'only digital' services and ecosystems and their new up-and-coming AI models and applications.

Competition authorities anchor their oversight in a static interpretation of market power, frequently transposing the winner-takes-most logic of legacy digital platforms onto the AI landscape. While they express valid concerns that data control creates barriers to entry, this perspective overlooks the dynamic complexities inherent in AI development, such as the volatility of model drift and the potential of within-user learning over traditional learning effects. By prioritizing fixed structural concerns over growing economic evidence, authorities inadvertently regulate based on a historical snapshot of platform dynamics.

III. A Review of the Regulatory Obligations Imposed on Digital Platforms

The paper identifies data asymmetries and learning effects in both traditional digital platforms and AI downstream markets and sets them apart, stemming from the available economic evidence on their impacts, noting unchallenged and contested studies that have dealt with the phenomenon.

Both notions guide regulators and competition authorities to reorient their enforcement strategies vis-à-vis AI providers of closed and dominant models. Greater attention has been drawn to the fact that competition authorities are currently exploring exploitative theories of harm to capture unfair conduct applied by AI dominant providers in downstream markets.

Notwithstanding, the paper turns its attention to an underexplored space: the *ex-ante* regulatory approach in competition policy directed at Big Tech companies crafting their proprietary and closed AI models. Under the assumption that antitrust rules lack effectiveness and the quick pace necessary to address the competitive problems originating from the business models and conduct of Big Tech digital platforms, *ex ante* regulations take a clear stance towards competitive advantages sustained on data, in that they should be undermined for the incumbent to level the competitive playing field.

Two sets of *ex ante* rules demonstrate this position: the EU's Digital Markets Act (DMA) and the British Digital Markets, Competition and Consumers Act (DMCCA).[109] The EU's regulatory approach prohibits regulatory targets from

[109] DMCCA, *supra* note 48. Other jurisdictions such as Turkey, Australia and Brazil also propose to apply similar rules to the processing of personal data, but the amendments to their competition law regimes have not yet been approved or entered into force, see Zeynep Ezgi Yanarateş, *Amendments in the Law on the Protection of Competition*, ERDEM & ERDEM (July 2020), https://www.erdem-erdem.av.tr/en/insights/amendments-in-the-law-on-the-

combining, cross-using, and processing personal data across their services and with first-party and/or third-party data.[110] The EU legislator drew its inspiration from cases that had formerly considered an anti-competitive harm derived from privacy infringements, notably the German competition authority's case against Meta's processing activities.[111]

The learning effects these regulatory targets formerly held remain impacted when they cannot combine personal data across their services. The increment in utility they derive from users joining the network on the platform will not yield substantial advantages for their data feedback loops. They cannot reap the benefits derived from the network. Learning effects taking place in their individual services remain untouched. In a similar vein, data asymmetries remain the same at the individual level, whereas they are grossly impacted by the regulatory obligation if one looks at the regulatory target's role as an ecosystem holder.

The British approach is more cautious. The DMCCA establishes that the British regulator may impose conduct requirements on regulatory targets captured by the *ex-ante* rules when they are found to be using data unfairly. Conduct requirements may apply to a broader or narrower set of actions performed by the regulatory targets captured by the DMCCA.[112] The CMA does not place restrictions

---

protection-of-competition; Alba Ribera Martínez, *A Fast Follower Ex-Ante Regime: Australia's Proposed New Digital Competition Regime*, KLUWER COMPETITION LAW BLOG (December 9, 2024), https://legalblogs.wolterskluwer.com/competition-blog/a-fast-follower-ex-ante-regime-australias-proposed-new-digital-competition-regime/; and Alba Ribera Martínez, *Brazil Seeks to Amend its Competition Law: A Regulatory Model à la Allemande*, KLUWER COMPETITION LAW BLOG (October 20, 2025), https://legalblogs.wolterskluwer.com/competition-blog/brazil-seeks-to-amend-its-competition-law-a-regulatory-model-a-la-allemande/. Despite that Japan also introduced ex ante digital rules on data processing, its focus did not revolve around such processing activities, as shown in Alba Ribera Martínez, *Japan's Mobile Software Competition Act Grows its Guidelines*, KLUWER COMPETITION LAW BLOG (October 6, 2025), https://legalblogs.wolterskluwer.com/competition-blog/japans-mobile-software-competition-act-grows-its-guidelines/.

[110] The DMA only hinders processing of personal data across services for the purposes of online advertising, DMA *supra* note 47, at Article 5(2)a.

[111] Friso Bostoen, *Understanding the Digital Markets Act*, 68 ANTITRUST BULL. 263, 263; Karsten K. Zolna, *The Law and Economics of Art. 5(2) DMA: The Case of Meta*, SSRN (September 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5424894; and Bundeskartellamt, Decision B6-22/11 of 6 February 2019.

[112] Both Google and Apple have been designated by the CMA as having strategic market status regarding their mobile platforms, see Notice Under Section 14(2) of the Digital Markets, Competition and Consumers Act 2024 (the Act), 22 October 2025 and Notice Under Section 14(2) of the Digital Markets, Competition and Consumers Act 2024 (the Act), 22 October 2025. The CMA also designated Google's strategic market status regarding its search services, see Competition and Markets Authority, *CMA Confirms Google Has Strategic Market Status in Search Services*, GOV.UK (October 10, 2025), https://www.gov.uk/government/news/cma-

on regulatory targets to share data within their ecosystems as a top priority. The British regulator points out the lack of economic evidence that these types of regulatory interventions outweigh the potential risks to innovation in digital markets.[113] The British regulator signals, to some extent, that economic evidence is not sufficiently uncontested to apply across-the-board regulatory solutions to end learning effects and asymmetries.

Furthermore, the wave of *ex ante* regulations targeting digital platforms and services has turned the tide in favor of capturing state-of-the-art technologies influencing the market outcomes of the digital space. The same regulators who enforce these regulatory obligations and remedies increasingly consider whether generative AI models should fall under the scope of their regulatory scrutiny.

On the EU side, the European Commission is reviewing the DMA's enforcement scope to establish whether AI should be included as a service meriting regulatory scrutiny.[114] The application of the prohibition on processing, combining, and cross-using data would set the functioning of AI models at odds with their intended function.[115] These provisions were designed to prevent gatekeepers from

---

confirms-google-has-strategic-market-status-in-search-services. At the moment of writing, the CMA has not imposed a single conduct requirement against them, see *The CMA's programme of work across mobile platforms*, GOV.UK (February 10, 2026), https://www.gov.uk/guidance/the-cmas-programme-of-work-across-mobile-platforms.

[113] The CMA fleshes out its priorities in terms of the DMCCA enforcement on its Roadmaps relating to what conduct requirements it expects to impose on Google and Apple, see, for instance, Strategic market status investigation into Google's general search services: Roadmap of possible measures to improve competition in search, 24 June 2025, paras. 3.32 and 3.33.

[114] Directorate-General for Competition & Directorate-General for Communications Networks, Content and Technology, *Commission Gathers Views on How the DMA Can Support Fair and Contestable Digital Markets and AI Sector*, DIGITAL MARKETS ACT (DMA) (August 27, 2025), https://digital-markets-act.ec.europa.eu/commission-gathers-views-how-dma-can-support-fair-and-contestable-digital-markets-and-ai-sector-2025-08-27_en. European Parliament representatives called for the inclusion of AI as a service meriting regulatory capture, as addressed in Alba Ribera Martínez, *Generative AI in Check: Gatekeeper Power and Policy under the DMA*, SSRN (December 6, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5025742; Jan-Frederick Göhsl, *Future Proofing the DMA for Agentic AI: Lessons from the AI Act*, 48 WORLD COMPET. 1, 10 (2025); and Friso Bostoen & Jan Krämer, *Is the DMA Ready for Agentic AI?* CERRE REPORT (July 2025), https://cerre.eu/wp-content/uploads/2025/07/Is-the-DMA-Ready-for-Agentic-AI_Final.pdf.

[115] For a broader analysis, see Alba Ribera Martínez, *The Regulation that Cried Wolf: Generative AI Training Data and the Challenge of Lawful Scale*, SSRN (May 6, 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5222181. On this same point, defending this same position, Bertin Martens, *How DeepSeek Has Changed Artificial Intelligence and What it Means for Europe*, BRUEGEL (March 20, 2025), https://www.bruegel.org/policy-brief/how-deepseek-has-changed-artificial-intelligence-and-what-it-means-europe.

leveraging data accumulated across one area of activity to entrench their position in adjacent markets. However, AI models are not merely consumers of data. They are dependent on the large-scale combination and cross-use of diverse data sources for pre-training, fine-tuning, and improvement through interaction data.

In the UK, the regulator concluded that AI features and functionalities fall right into the regulation's scope, despite its lack of an appetite for imposing regulatory obligations that address learning effects and asymmetries. The CMA recognized that AI-based search features such as AI Overviews and AI Mode were confirmed as falling within the scope of the DMCCA's application. Notwithstanding, Google's Gemini AI assistant was excluded on the basis that its current usage is distinct from general search, with the CMA noting it will keep this position under review as the market develops. Data dynamics specific to foundation model development, including data flywheels and learning effects, currently fall outside of the DMCCA's operative perimeter.[116]

If one applies the DMA's underlying rationale, an AI provider cannot combine data to power and train its AI model.[117] Negative externalities as adverse selection stemming from data asymmetries will remain untouched. Path dependencies deriving from within-user learning constitute the core of the negative externalities of learning effects in AI downstream markets. Those especially happen in targeted learning, where the AI model learns about a specific user's interactions and responses to the service and locks the consumer in a recursive feedback loop. The DMA's regulatory prohibition impacts the available resources to the regulatory target, creating diminishing returns that can lead the AI model to underfitting and, necessarily, to lowering its utility. Even though the regulatory target still enjoys the benefits of within-user learning and third parties suffer their consequences, the regulatory transformation addresses the super-additive outcomes influencing improvements in across-user learning. The competitive playing field is indeed levelled, but at a lower point of utility.

The DMA's rigid approach to data siloing inadvertently validates the British regulator's caution by inducing model underfitting and capping the utility of generative AI. By preventing gatekeepers from aggregating data across their designated services, the regulation confines the model's training to service-specific

[116] Competition and Markets Authority, *supra* note 66.

[117] Regulatory targets such as Meta have done just that to power their AI models by scraping data from their services and combining it to improve their current AI offerings, see Jacob Wulff Wold, *Meta Reverts to AI Training on Facebook and Instagram Posts Despite Legal Pushback*, EURACTIV (April 14, 2025), https://www.euractiv.com/news/meta-resumes-ai-training-on-facebook-and-instagram-posts-after-legal-pushback/.

datasets that are necessarily narrower and less representative than the cross-platform data infrastructure that current state-of-the-art models require.

In short, the DMA transforms the trajectory of learning effects from a recursive feedback loop to a siloed and hyper-local feedback loop capped per service. Learning effects will only be enjoyed within the boundaries of each individual AI model's designated service context, without the service's capacity to train and re-train data coming from different sources. The model's capacity for across-user learning is directly curtailed, even as within-user learning continues uninterrupted within each service silo. In short, undertakings wishing to train and deploy their services in the market face outright impediments to growing their models.

IV. Applicable Computational Presumptions to Learning Effects and Asymmetries

Assuming the impact of these regulatory obligations on consumer-facing model utility and their lack of an impact regarding data asymmetries, the paper proposes an alternative approach towards tackling learning effects and asymmetries by presenting an additional instrument to the regulator's toolkit: the application of computational techniques.

Competition authorities integrate these tools into their daily enforcement of antitrust prohibitions,[118] but they have seldom explored the possibilities they hold in automating compliance with regulatory requirements.[119] The literature has proposed to temper the effects of data asymmetries[120] and learning effects[121] via the

[118] For a fully-fledged review see Schrepel & Groza, *supra* note 52.

[119] Such a proposal is addressed in Herwig C.H. Hofmann & Isabella Lorenzoni, *Future Challenges for Automation in Competition Law Enforcement*, 3 STAN. COMPUT. ANTITRUST 36, 45 (2023); and Jay L. Himes, Jason Nieh & Ron Schnell, *Antitrust Enforcement and Big Tech: After the Remedy Is Ordered*, 1 STAN. COMPUT. ANTITRUST 64, 66-70 (2021).

[120] In the field of differential privacy, see Michael Khavkin & Eran Toch, *Investigating the Impact of Differential Privacy Obfuscation on Users' Data Disclosure Decisions*, 196 DECIS. SUPPORT SYST. 114474, 114482 (2025). For federated learning, see Hongliu Cao, *Holistic Analysis On the Sustainability of Federated Learning Lifecycle In Real-World Industrial Settings*, ARXIV (July 16, 2025), https://doi.org/10.48550/arXiv.2312.14628; and Justin Curl & Xing Xie, *Societal Impacts and Opportunities of Federated Learning*, 11 CHIN. J. SOCIOL. 90, 95 (2025). Finally, on multi-party computation, see Wirawan Agahari, Hosea Ofe, Mark de Reuver, *It Is Not (Only) About Privacy: How Multi-Party Computation Redefines Control, Trust, and Risk in Data Sharing*, 32 ELECTRON. MARK. 1577, 1581 (2022).

[121] In the case of synthetic data, see Michal S. Gal & Orla Lynskey, *Synthetic Data: Legal Implications of the Data-Generation Revolution*, 109 IOWA L. REV. 1087, 1092 (2024); Rozhina Ghanavi & Catherine E. Tucker, Synthetic Data, *Network Effects, and the Future of Competition*, COMPETITION POLICY INTERNATIONAL (October 23, 2025), https://www.pymnts.com/cpi-posts/synthetic-data-network-effects-and-the-future-of-competition/. For differential privacy, see Yuan Luo & Nicholas R. Jennings, *A Differential Privacy Mechanism that Accounts*

application of computational tools. Even when authors differ on the computational techniques to be introduced,[122] the literature suggests they can move the competitive moat away from the mere possession of raw data.

The main practical hurdle to turning these computational techniques into compliance mechanisms of *ex ante* regulation is that they are not designed with these objectives in mind. Instead, the most advanced sets of computational techniques addressing data flows have been traditionally developed to satisfy the legal requirements of privacy.

Privacy-preserving computation provides techniques and tools to perform computations and data analysis while preserving data confidentiality.[123] Depending on their purpose and form, two distinct types of computation tools emerge: obfuscation and cryptographic tools.[124] Obfuscation tools mask data by either creating a synthetic form of text that bears the same characteristics as the original dataset (synthetic data[125]) or by encrypting the underlying data (differential

for Network Effects for Crowdsourcing Systems, 69 J. ARTIF. INTELL. RES. 1127, 1127 (2020). For federated learning, see Joaquin Delgado Fernandez, Martin Brennecke, Tom Barbereau, Alexander Rieger & Gilbert Fridgen, *Federated Learning: Organizational Opportunities, Challenges and Adoption Strategies*, ARXIV (September 6, 2023), https://doi.org/10.48550/arXiv.2308.02219.

[122] Some authors argue that applying differential privacy, which provides strong privacy protections, misaligns with user preferences. Users tend to prefer being compensated by larger rewards at an increased privacy risk, see Khavkin & Toch, *supra* note 120, at 114494-114495. Luo & Jennings, *supra* note 121, at 1127-1128 highlight that a unique equilibrium must be considered, given that some users might be incentivized to protect their data in this way, whereas others might want to reap their rewards by participating of the advantages of learning effects. Other authors defend that multi-party computation prevents losing competitive advantages for economic players due to data leakage whilst it creates new risks of data misuse, see Agahari, Ofe & de Reuver *supra* note 120, at 1577. In the analysis of synthetic data, several authors defend that it can significantly reduce access barriers to data when reducing privacy and data security breaches, see Gal & Lynskey, *supra* note 121, at 1154-1155. Opposing opinions are held by Curl & Xie, *supra* note 120, at 94 by stating that federated learning is a potential remedy for countering economic concentration, but it must first overcome several technical challenges before achieving widespread adoption.

[123] Aitor Gómez-Goiri, Iñaki Seco-Aguirre, Oscar Lage & Alejandra Ruiz, *Privacy-Preserving Computation Meets Quantum Computing: A Scoping Review*, DIGIT. COMMUN. NETW. 1, 1 (2025).

[124] OECD, *Sharing Trustworthy AI Models with Privacy-Enhancing Technologies*, OECD ARTIFICIAL INTELLIGENCE PAPERS NO. 38 (2025), https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/06/sharing-trustworthy-ai-models-with-privacy-enhancing-technologies_5df6fd05/a266160b-en.pdf.

[125] Synthetic data is artificial data that is generated from original data and a model that is trained to reproduce the characteristics and structure of the original data. Definition extracted from Robert Riemann, *Synthetic Data*, EUROPEAN DATA PROTECTION SUPERVISOR, https://www.edps.europa.eu/press-publications/publications/techsonar/synthetic-data_en.

privacy[126]). Cryptographic tools make data unreadable to ensure confidentiality and integrity by using mathematical algorithms and secret keys, such as homomorphic encryption,[127] multi-party computation,[128] federated learning,[129] and trusted execution environments.[130] None of these computational techniques acts as a silver bullet to protect privacy in every context whilst preserving the utility of the underlying data. As a matter of fact, firms cluster their approaches by integrating different computational techniques into a single framework to cover different aspects of data confidentiality.

Nearly all kinds of cryptographic techniques can interact with RLHF to counter the privacy risks generated by data inputted by the consumer and later fed into the model.[131] When data utility may be preserved whilst neutralizing privacy risks, learning effects still prevail. There is a positive correlation between the deployment of these computational techniques and their prevalence.

---

[126] Differential privacy is a privacy-preserving technique that conceals individual data points in a dataset by adding controlled random noise. Derived from Chenhao Xu, Youyang Qu, Yong Xiang & Longxiang Gao, *Asynchronous Federated Learning on Heterogeneous Devices: A Survey*, 50 COMPUT. SCI. REV. 100595, 100598-100599 (2023).

[127] Homomorphic encryption is a cryptographic construction allowing an application to operate on encrypted data, instead of the raw data itself. Definition extracted from Vitor Falcao da Rocha & Julio López, *An Overview on Homomorphic Encryption Algorithms*, STATE UNIVERSITY OF CAMPINAS INSTITUTE OF COMPUTING (2018), https://ic.unicamp.br/~reltech/PFG/2018/PFG-18-28.pdf.

[128] Secure multi-party computation is defined as a secure protocol allowing multiple participants to collaboratively compute an objective function using their private inputs while ensuring that each participant only receives their corresponding output, thus preserving privacy. Derived from Ziqin Chen & Yongjian Wang, *Privacy-Preserving Distributed Optimization and Learning*, 36 ENCYCLOPEDIA OF SYSTEMS AND CONTROL ENGINEERING 308, 308 (2025).

[129] Federated learning develops machine-learning models where each federated device shares its local model parameters instead of sharing the whole dataset used to train it. Definition extracted from Xabier Lareo, *Federated Learning*, EUROPEAN DATA PROTECTION SUPERVISOR, https://www.edps.europa.eu/press-publications/publications/techsonar/federated-learning_en.

[130] A trusted execution environment is an environment using hardware-backed techniques to provide increased security guarantees for the execution of code and protection of data within that environment. Definition extracted from The Confidential Computing Consortium, *Confidential Computing: Hardware-Based Trusted Execution for Applications and Data*, CONFIDENTIAL COMPUTING (2022), https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC_outreach_whitepaper_updated_November_2022.pdf.

[131] For an example of these approaches, see Bian Zhu & Ling Niu, *A privacy-preserving federated learning scheme with homomorphic encryption and edge computing*, 118 ALEX. ENG. J. 11 (2025). For a comprehensive account of their interaction, see Nouha Oualha, SoK: *Privacy-Enhancing Technologies in Artificial Intelligence*, ARXIV (June 17, 2025), https://doi.org/10.48550/arXiv.2506.14576.

Computational techniques do not substantially impact an existing AI model's prediction capabilities regarding across-user learning because encrypted and obscured data will still derive the general characteristics of consumers inserted in the stages of its development. Learning effects driving the model's improvement due to the number of consumers enjoying it will still apply to the overall user base.

Traditionally, synthetic data is assumed to be the most apt to counter learning effects. It is used in training to replicate entire datasets and can, therefore, allow new entrants to achieve high model performance without a massive initial user base.[132] Mixed evidence points to the fact that models predominantly trained on synthetic data may lead to model collapse, because of reduced diversity or amplified biases.[133] Other types of cryptographic tools deliver better results when applied in isolation. When differential privacy is applied to RLHF, privacy guarantees come at almost no drop in data utility.[134] Federated analysis can also play a significant role, since it reduces the need for large-scale data transfers. AI models process data locally on user devices instead of sending data to a central server for analysis. Only the processed results or outputs will be transmitted to the central location for reinforcement learning.[135]

Notwithstanding, these same tools bring consequences for within-user learning, which might be more limited when AI providers cannot offer highly targeted, personalized offerings and service improvements to the most engaged users

---

[132] Empirical work has been produced to this effect, see Pratyush Maini, Vineeth Dorna, Parth Doshi, Aldo Carranza, Fan Pan, Jack Urbanek, Paul Burstein, Alex Fang, Alvin Deng, Amro Abbas, Brett Larsen, Cody Blakeney, Charvi Bannur, Christina Baek, Darren Teh, David Schwab, Haakon Mongstad, Haoli Yin, Josh Wills, Kaleigh Mentzer, Luke Merrick, Ricardo Monti, Rishabh Adiga, Siddharth Joshi, Spandan Das, Zhengping Wang, Bogdan Gaza, Ari Morcos & Matthew Leavitt, *BeyondWeb: Lessons from Scaling Synthetic Data for Trillion-Scale Pretraining*, ARXIV (August 19, 2025), https://doi.org/10.48550/arXiv.2508.10975. In its relationship with competition, see Ghanavi and Tucker, *supra* note 121.

[133] Defending their theory on model collapse, see Elvis Dohmatob, Yunzhen Feng, Arjun Subramonian & Julia Kempe, *Strong Model Collapse*, ARXIV (October 8, 2024), https://doi.org/10.48550/arXiv.2410.04840; and Ilia Shumailov, Zakhar Shumaylov, Yiren Zhao, Yarin Gal, Nicolas Papernot & Ross Anderson, *The Curse of Recursion: Training on Generated Data Makes Models Forget*, ARXIV (April 14, 2024), https://doi.org/10.48550/arXiv.2305.17493. For a more nuanced account about the likelihood of model collapse, Feiyang Kang, Newsha Ardalani, Michael Kuchnik, Youssef Emad, Mostafa Elhoushi, Shubhabrata Sengupta, Shang-Wen Li, Ramya Raghavendra, Ruoxi Jia & Carole-Jean Wu, *Demystifying Synthetic Data in LLM Pre-Training: A Systematic Study of Scaling Laws, Benefits and Pitfalls*, ARXIV (October 2, 2025), https://doi.org/10.48550/arXiv.2510.01631.

[134] Dan Qiao & Yu-Xiang Wang, *Offline Reinforcement Learning with Differential Privacy*, ARXIV (January 3, 2023), https://doi.org/10.48550/arXiv.2206.00810.

[135] CENTRE FOR INFORMATION POLICY LEADERSHIP, PRIVACY-ENHANCING AND PRIVACY-PRESERVING TECHNOLOGIES IN AI: ENABLING DATA USE AND OPERATIONALIZING PRIVACY BY DESIGN AND DEFAULT (2025).

in the network based on insights derived from their own interactions with the AI model. Bearing in mind that the underlying data is obscured or encrypted, AI providers will hardly possess feasible mechanisms to retain these high-value users feeding on within-user learning. This dynamic may open these segments of the market to competition that has grown loose of pre-existing barriers to entry and expansion. By lowering lock-in effects for those consumers via these means, those consumers will be more likely to switch to a competitor because the scale of learning is less path-dependent, as opposed to the scenario where they exhibit compounding switching costs in the AI market.[136]

Under the premise that an existing incumbent drives negative externalities onto third parties via within-user learning, the application of any of these computational techniques should, at least, merit the regulator's consideration. The force of computational presumptions can be introduced at this point to alleviate the workload of competition authorities and regulators alike and square the circle of an AI model's deployment with the DMA's application to it. Undertakings that can prove that the deployment of the computational technique of their choice reaches the adequate privacy-utility trade-off whilst eliminating the negative externalities of within-user learning merit being held to account in line with a safe-harbor like threshold.

Bearing in mind that data inputted by the user is not too sensitive (including, for example, medical and financial information), the US National Institute of Standards and Technology establishes that the acceptable threshold indicating that the AI provider preserves data utility whilst sufficiently obscuring data embedded in the AI model is that of $2 < \varepsilon < 8$.[137]

ε (or epsilon) is a core parameter quantifying privacy loss. A smaller epsilon ($\varepsilon < 1$) means more noise has been added to the data, and data utility decreases with it.[138] A larger epsilon ($\varepsilon > 1$) allows for more utility but less privacy, ensuring the overall impact on an individual's privacy remains within acceptable bounds. A higher ε entails that the AI provider will have a higher privacy budget. An individual's specific data will have a greater impact when ε remains higher. $\varepsilon > 10$ means that an attacker

[136] Hagiu & Wright, *supra* note 84, at 7.

[137] JOSEPH P. NEAR, DAVID DARAIS, NAOMI LEFKOVITZ & GARY S. HOWARTH, GUIDELINES FOR EVALUATING DIFFERENTIAL PRIVACY GUARANTEES (2025).

[138] As proved in Alexandra Wood, Micah Altman, Aaron Bembenek, Mark Bun & Marco Gaboardi, *Differential Privacy: A Primer for a Non-Technical Audience*, 21 VAND. J. ENT. & TECH. L. 209, 209 (2018).

is over twenty-two thousand times more likely to learn something about an individual compared to if they had never seen the data.[139]

Presuming that anti-competitive harms caused by learning effects will rarely materialize because super-additive impacts flowing from within-user to across-user learning have been eliminated, regulatory targets cannot be simply excluded from re-training their models altogether, as expected by the DMA.

In those cases where the AI provider can prove that $2 < \varepsilon < 8$, the regulatory presumption of compliance with the DMA can apply. Regulators can certainly adjust the thresholds that seem acceptable within the privacy-utility trade-off to ensure that an AI provider's learning effects are sufficiently removed. Where AI providers instead rely on federated learning or homomorphic encryption (that lack a native ε parameter), compliance with the computational presumption shall be assessed by reference to functionally equivalent measurable indicators, such as the model's empirical reconstruction error rate[140] or the guaranteed indistinguishability bound[141] under the chosen cryptographic scheme.

The regulatory presumption would operate to offer legal certainty to AI providers and reduce compliance costs for the regulator. Computational presumptions come to the rescue by creating a safe harbor space where they are *prima facie* exempted from complying with the prohibition on data combinations and

---

[139] Priyanka Nanayakkara, Mary Anne Smart, Rachel Cummings, Gabriel Kaptcuk & Elissa M. Redmiles, *What Are the Chances? Explaining the Epsilon Parameter in Differential Privacy*, 91 SEC'23: PROCEEDINGS OF THE 32ND USENIX CONFERENCE ON SECURITY SYMPOSIUM 1613, 1613-1615 (2023). Larger values of ε do not always provide meaningful real-world privacy, as set out in Damien Desfontaines, *A list of real-world uses of differential privacy* (October 1, 2021), https://desfontain.es/blog/real-world-differential-privacy.html; Andrea Gadotti, Florimond Houssiau, Meenatchi Sundaram Muthu Selva Annamalai & Yves-Alexandre de Montjoye, *Pool Inference Attacks on Local Differential Privacy: Quantifying the Privacy Guarantees of Apple's Count Mean Sketch in Practice*, 31ST USENIX SECURITY SYMPOSIUM 501, 501 (2022); Theresa Stadler, Bristena Oprisanu & Carmela Troncoso, *Synthetic Data – Anonymisation Groundhog Day*, 31ST USENIX SECURITY SYMPOSIUM 1451, 1451 (2022); and Milad Nasl, Shuang Songi, Abhradeep Thakurta, Nicolas Papemoti & Nicholas Carlin, *Adversary Instantiation: Lower Bounds for Differentially Private Machine Learning*, IEEE SYMPOSIUM ON SECURITY AND PRIVACY 866, 866 (2021).

[140] This methodology has been backed by Samaneh Mohammadi, Ali Balador, Sima Sinaei & Francesco Flammini, *Balancing privacy and performance in federated learning: A systematic literature review on methods and metrics*, 192 J. PARALLEL. DISTR. COM. 104918, 104918-104942 (2024); and Shangyin Weng, Yan Gou, Lei Zhang & Muhammad Ali Imran, *Evaluating privacy loss in differential privacy based federated learning*, 172 FUTURE GENER. COMPUT. SYST. 107848, 107848-107868 (2025).

[141] As noted in Amr Alanwar, Victor Gaßmann, Xingkang He, Hazem Said, Henrik Sandberg, Karl H. Johansson & Matthias Althoff, *Privacy-preserving set-based estimation using partially homomorphic encryption*, 71 EUR. J. CONTROL. 100786, 100786-100806 (2023).

cross-use, whilst maintaining barriers to entry and expansion to AI downstream markets at bay.

When one turns to data asymmetries, the establishment of computational presumptions proves more challenging. Implementation of federated learning or homomorphic encryption directly excludes access to data to AI providers. Having lowered the disparity of data access, under the guiding principles of these computational tools, the black box problem blinds all involved parties within the transaction. AI providers and consumers stand on an equal footing in terms of the valuations they assign to the consumer sharing their data with the service, because they both lack enough information to perform it. Not transparency, but more opacity, generated through the application of computational techniques, leads to a lower probability of resource misallocation taking place. In a similar vein to the computational presumption applying to learning effects, an equivalent can be simply derived from this scenario. Here, introducing thresholds according to privacy-utility trade-off is not even relevant, but a stronger presumption will necessarily apply when it approximates $\varepsilon < 1$. This is a robust threshold that entails strong privacy protection and, therefore, visibility on consumer needs and wants remains obscured. A symmetric lack of information applies to the framework, and adverse selection will not materialize as a negative externality.

Some authors, however, have pointed out that asymmetries will still prevail in traditional digital markets since the service providers of these cryptographic tools are largely the same as the incumbent digital platforms.[142] Current implementations of cryptography, thus, aim to counteract external threats posed by third parties but not to extinguish the service providers' threats.[143] The conflation of service providers remains, thus, a crucial factor that the application of a potential regulatory presumption should take into account. When incumbent players remain in control of their own cryptographic tools, it will be less likely that those mechanisms will contribute to narrowing the data asymmetries they have generated themselves.

Regulatory presumptions cannot be applied in the full range of scenarios outlined throughout the paper. The paper's limitations sketch out a broader research agenda for the future. Even though these computational techniques, in appearance, reduce data asymmetries since AI providers and developers access low levels of personal data from the consumer, the black-box problem is not yet resolved, both

---

[142] Alessandra Calvi, Gianclaudio Malgieri & Dimitris Kotzinos, *The Unfair Side of Privacy Enhancing Technologies: Addressing the Trade-Offs Between PETs and Fairness*, FACCT'24: PROCEEDINGS OF THE 2024 ACM CONFERENCE ON FAIRNESS, ACCOUNTABILITY AND TRANSPARENCY 2047, 2054-2055 (2024).

[143] Ero Balsa, Helen Nissenbaum & Sunoo Park, *Cryptography, Trust and Privacy: It's Complicated*, CSLAW'22: PROCEEDINGS OF THE 2022 SYMPOSIUM ON COMPUTER SCIENCE AND LAW 167, 167 (2022).

technically and legally. One cannot simply assert that data asymmetries disappear into thin air because personal data will not abound in the presence of computational techniques.

A clear finding emerges from the paper's discussion. The introduction of a computation presumption establishing a safe harbor threshold, such as the NIST-aligned $2 < \varepsilon < 8$, can aid regulators in automating compliance with *ex ante* regulations by demonstrating a substantial decrease in the impact of within-user learning without stifling the utility of AI models.

By integrating computational presumptions of this type into the antitrust toolkit, regulators can move beyond behavioral bans towards an architectural enforcement model. This approach transforms privacy-preserving tools from mere shields countering privacy risks into active instruments of market contestability. Integrating these types of computational presumptions into the regulator's toolkit allows for a more nuanced enforcement of *ex ante* regulations by replacing the blunt prohibition on data usage with a framework that balances the preservation of contestable markets with the necessity of maintaining competitive and entry-ready AI downstream markets.

V. The Challenges of Implementation

Transforming computational techniques into tractable instruments of legal and regulatory decision-making is easier said than done. Regulators will have to accommodate engaging with highly sophisticated tools whilst ensuring that they preserve the spirit and letter of the laws they are applying.

The proposal to introduce safe harbor thresholds seeks to simplify the immense task ahead of regulators relating to how they capture the phenomenon of AI via their existing *ex ante* obligations. As it currently stands, the regulatory prohibitions on data combinations compel regulators to monitor all data flows across a regulatory target's ecosystem. Since no illicit data combinations must take place, regulators are forced to track data flows and set apart which combinations should not be allowed as a rule, stemming from the regulatory target's data infrastructure.

Performing such an exhaustive task is akin to the task of looking for a needle in a haystack. Even though monitoring data in real-time for Big Data systems has improved immensely during the last decade,[144] the sheer volume of data that Big Tech operations would entail poses several challenges. Unprecedented data volumes can exceed the limits of reliable processing and storage needed for tracking these wide-

[144] Ikram Lefhal Lalaoui, Essaid El Haji & Mohamed Kounaidi, *The Evolution and Challenges of Real-Time Big Data: A Review*, 10 COMPUT. SCI. MATH. FORUM 11, 11 (2025).

spanning data flows.[145] The absence of standardized data formats and the low interoperability of processing platforms may limit the scalability and integration of these solutions.[146] Tracking systems tend to underperform when multiple data sources are aggregated,[147] and this is precisely what they would be forced to do if the regulatory obligations were to be complied with in the strictest of senses. In the case of Big Tech players, data flow mapping can be fraught with challenges due to the intricate network of systems and data streams involved.[148]

The paper proposes to abandon the quest for needles in the haystack by implementing a straightforward solution that considers high-precision computational techniques that, once implemented, can prove to be easy to manage for regulators. Under the paradigm of computational presumptions, regulators can audit a single value and test it with automated tools, without the need to conduct ongoing and real-time monitoring of all regulatory target's data flows that, in the end, are resource-intensive and may not deliver on desired results.

The nature of computational presumptions draws on the tradition of antitrust enforcement in relying on safe harbor thresholds when undertakings self-assess the conduct they perform in the market. As a result of developments in economic theory, the way antitrust treats certain practices have changed.[149] For instance, the application of antitrust rules in some jurisdictions has rehabilitated prohibited practices as being mainly pro-competitive.[150]

The importance of safe harbors displays prominently within this trove of instruments that competition authorities and regulators are increasingly using to shape antitrust enforcement.[151] Safe harbor refers to mechanisms that make it

---

[145] As shown in Wei Xu, Ying Cao & Runyu Chen, *A multimodal analytics framework for product sales prediction with the reputation of anchors in live streaming e-commerce*, 177 DECIS. SUPPORT SYST. 114104, 114104 (2023).

[146] Providing evidence of such an effect, see Paweł Macias, Damian Stelmasiak & Karol Szafranek, *Nowcasting food inflation with a massive amount of online prices*, 39 INT. J. FORECAST. 809, 809 (2023).

[147] These were some of the impacts registered in Theofanis P. Raptis, Claudio Cicconetti & Andrea Passarella, *Efficient topic partitioning of Apache Kafka for high-reliability real-time data streaming applications*, 154 FUTURE GENER. COMPUT. SYST. 173, 173 (2024).

[148] Brent Huston, *The Challenges and Need for Data Flow Mapping*, STATE OF SECURITY (March 3, 2025), https://stateofsecurity.com/the-challenges-and-need-for-data-flow-mapping/.

[149] As a matter of fact, some authors defend that safe harbors have not been mainstream in antitrust enforcement since the turn of the century, Lindsey M. Edwards & Joshua D. Wright, *The Death of Antitrust Safe Harbors: Causes and Consequences*, 23 GEO. MASON L. REV. 1205, 1250 (2016).

[150] Daniel A. Crane, *Rules Versus Standards in Antitrust Adjudication*, 64 WASH. & LEE L. REV. 49, 51-52 (2007).

[151] For a detailed account of the toolkit, see Secretariat of the OECD, SAFE HARBOURS AND LEGAL PRESUMPTIONS IN COMPETITION LAW (2017).

harder to establish liability for certain business practices, and that is precisely what the epsilon-reliant thresholds provide for regulated targets. They can avoid liability under the *ex-ante* regulatory regimes when they can prove that they meet those thresholds to the requisite legal standard.

Due to the multiplicity of scenarios that regulators must face when regulatory targets deploy and develop their AI models, the adoption of safe harbor thresholds ensures the administrability of these rules on two different fronts. Regulatory targets can provide their services in the market with certainty, without facing the risk of an infringement looming over their heads. Regulators avoid the expenditure of resources by assessing the potential impact of such practices in the regulatory regimes.[152]

In practice, the proposed safe harbor epsilon-reliant thresholds do not operate in the form of a substantive presumption of legality akin to those in antitrust enforcement, because conduct takes place in the framework of the regulatory iterations between regulated targets and regulators. Regulatory targets must prove that they adhere to a given rule (in this case, a prohibition), but it can choose how it prefers to do so. The safe harbor legal thresholds pave the way in this direction and provide a clear fix for regulatory targets to act on. They can optimize their AI models to converge with the safe harbor so that regulatory compliance is more manageable and more easily auditable.

Instead of an antitrust substantial presumption, it represents a computational (regulatory) presumption of compliance. In case the regulatory targets satisfy the safe harbor, then the absence of a heavy-handed and widespread scrutiny over their AI models regarding the data combination ban should follow. However, the application of the threshold does not automatically mean that the regulatory target is completely out of the woods in terms of the regulatory requirements it must meet. The epsilon-based standard seeks to reduce the monitoring costs and provide the certainty that AI providers crave, but it is not a *carte blanche* that ensures regulatory compliance in each and every case.

For the safe harbor to deliver on its objectives, its implementation must be paired with automated and real-time auditing, ensuring that regulatory targets do not comply with the regulatory obligations in a single iteration, but rather that compliance is continuous and long-standing. The regulator could accommodate two distinct types of monitoring. On one hand, a continuous auditing of the models that flag deviations in real-time, or, on the other hand, a periodic monitoring that accounts for the AI models' memorization.

[152] Crane, *supra* note 150, at 99.

In the first case, real-time API auditing can be made available to identify compliance failures instantly, relating to data combinations, i.e., which user or system is accessing data, the endpoints, or the access type to the data. Audit logs would reflect breaches of the data combination ban, which would involve not only broader policy decisions taken by the regulatory targets that may infringe the regulatory obligation, but also smaller and sporadic deviations that can result in equally harmful results.

For the latter case, regulatory intervention would be sparsely needed in the absence of continuous monitoring. Regulators could place random and strategically placed auditing periods when engineers (or even third parties) would perform membership inference attacks[153] on the AI models to probe whether they have memorized specific examples of data provided to them as feedback signals. In case those certification efforts result in a contested case where leaks are flagged, then the regulator would then engage in a further forensic investigation involving access to the training and reinforcement learning pipelines that feed the AI model. Rather than looking for the needle in the haystack, the regulator would be checking the regulatory target's compliance with the law with verifiable properties in mind, so that factchecking and monitoring are much easier to perform and less resource-intensive than the unmanageable monitoring of all data flows.

The success of the epsilon-reliant safe harbors hinges on the synergy between legal certainty and technical rigor. While they offer a clear path for companies to optimize their models towards compliance, they must be underpinned by a clear auditing strategy, either that leverages real-time API checks or the depth of membership inference attacks. By doing so, regulators can ensure that the spirit of the *ex-ante* regulatory obligations remains intact without being crushed by the sheer weight of the data it seeks to govern.

VI. Conclusions

The paper has demonstrated that data asymmetries and learning effects in AI downstream markets do not follow the same trajectories that regulators have mapped onto traditional digital platforms. The nuance of within and across-user learning provides the justification of such a difference between both digital worlds.

Regardless of the gap, regulators seek to apply *ex ante* regulatory obligations that impose a ban on data combinations on AI markets. Those prohibitions will not

[153] Membership inference attacks can be performed by attackers (i.e., engineers) to determine if specific data points were included in the AI model's training, fine-tuning, alignment and reinforcement learning. For a review of the existing literature, see Hengyu Wu & Yang Cao, *Membership Inference Attacks on Large-Scale Models: A Survey*, ARXIV (August 31, 2025), https://doi.org/10.48550/arXiv.2503.19338.

capture the multi-faceted dimensions of across-user and within-user learning. When applied to AI markets, they will level the competitive playing field at a lower point of utility without resolving the consumer harm that motivated the regulatory intervention in the first place.

Against this framework, the paper's proposal strives to make the goals of *ex ante* regulation achievable in the context of AI markets. Computational presumptions grounded in verifiable privacy-utility thresholds transform the regulator's task from tracking every prohibited data combination across a gatekeeper's ecosystem to auditing a single and measurable parameter. The result is a framework that takes the competitive dynamics of AI downstream markets on their own terms.