The Seybold Report

ISSN 1533-9211

DOI: 10.5281/zenodo.20588248

THE STRUCTURAL IMBALANCE OF COMPETITIVE DYNAMICS IN E-COMMERCE PLATFORMS UNDER AI AGENT INTERVENTION AND THE RECONSTRUCTION OF LEGAL REGULATION

TING HOU[1*] and XIANG LI[2]

[1]2nd Year Undergraduate Student, The School of Publishing, University of Shanghai For Science and Technology, Majoring in Publishing And Editing. *Corresponding Author Email: tinghou1518@outlook.com
[2]Lecturer and Master's Supervisor, Department of Publishing and Digital Communication, School of Publishing, University of Shanghai for Science and Technology. Email: leeyouchrng@163.com

Abstract

Generative artificial intelligence–driven AI agents, characterized by cross-platform orchestration, autonomous decision-making, and task-planning capabilities, are fundamentally reshaping the competitive structure of e-commerce platforms. The traditional decision-making pathway—user, platform, and product—is increasingly transitioning toward a distributed architecture involving users, AI agents, and multiple platforms. In this emerging configuration, platform-centric advantages in entry control, traffic allocation, and data aggregation are significantly weakened, while the core of market competition shifts from intra-platform dynamics to algorithm-mediated intermediation. This paper conceptualizes AI agents as quasi-market actors and examines their structural challenge to platform governance power. It identifies several systemic tensions, including conflicts over gateway control, frictions between data governance and personal information protection, distortions in algorithmic decision authority, and the fragmentation of multi-actor responsibility frameworks. These dynamics collectively contribute to a reconfiguration of digital market power and regulatory uncertainty. To address these challenges, the paper proposes a set of governance reconstruction pathways. These include the establishment of auditable API access systems for platform entry control, the development of behavioral data authorization pools to regulate data circulation, the implementation of recommendation influence labeling mechanisms to enhance algorithmic transparency, and the construction of a segmented liability framework along the decision chain. This framework differentiates responsibilities across data generation, recommendation processing, and transaction execution stages. Through these institutional designs, the study aims to preserve technological innovation while redefining the power boundaries among platforms, AI agents, and users, thereby safeguarding fair competition in digital markets.

Keywords: AI Agents; e-Commerce Platforms; Algorithmic Governance; Data Circulation; Legal Liability Allocation.

1. INTRODUCTION

The advent of generative artificial intelligence and its progression into the era of large models has triggered profound transformations in the operational structure of the digital economy. AI systems have gradually transcended their traditional role in information retrieval, acquiring advanced capabilities in task planning, data integration, automated decision-making, and cross-platform invocation. AI agents, exemplified by systems such as Perplexity AI and Open AI Operator, can now independently perform product screening, price comparison, review analysis, and the generation of consumption recommendations. Consequently, the user decision-making pathway is evolving from a triadic structure of user–platform–product into one of user–AI agent–multiple platforms. The long-standing gatekeeping advantages that

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.20588248

platforms have derived from search ranking, traffic allocation, and data aggregation are being challenged, while the core of market competition is shifting from intra-platform rivalry toward competition among algorithmic intermediaries. As AI agents become deeply embedded in consumer decision-making, the emergent competition between platforms and algorithms over gatekeeping control, data utilization, and recommendation authority is becoming a critical issue in digital market governance.

Research on the governance of AI agents has proliferated in response to these developments. Large platforms' control over interfaces and data resources has assumed characteristics of digital infrastructure1. By imposing interface restrictions and differentiated access configurations, platforms may exclude external AI systems, potentially establishing new structural exclusionary mechanisms. This perspective has brought fair access issues into competition law discourse; however, scholarly attention remains predominantly focused on platforms' obligations to open their systems, with insufficient examination of the competitive functions performed by AI agents as independent market gateways2). Generative AI is already reshaping the structure of consumer choice, with algorithmic outputs increasingly exercising a "quasi-governance" function. Traditional consumer protection frameworks struggle to address the novel risks arising from automated decision-making systems. As generative AI assumes functions of information filtering and resource allocation, existing transparency obligations and risk-classification mechanisms within artificial intelligence regulatory frameworks require further extension to AI agent scenarios3). Algorithms are progressively becoming significant mechanisms influencing resource allocation and public order, necessitating a shift in future governance priorities from mere risk prevention toward structural governance4).

Domestic scholarship has similarly begun to address the disruptive impact of AI agents on platform order. Algorithmic systems have evolved from technical tools into influential institutional forces shaping market order. Platforms mold user behavioral pathways through algorithmic mechanisms, requiring legal regulation to focus on the underlying structural control capacities of algorithms5). Data circulation regimes must establish a dynamic equilibrium between personal information protection and data utilization; a singular emphasis on data control logic is ill-suited to the demands of data collaboration in the artificial intelligence era6).The recommendation mechanisms of generative AI are beginning to substitute for aspects of user judgment. Traditional frameworks of informed consent and platform liability are inadequate for scenarios involving AI autonomous decision-making, calling for algorithmic governance to advance from static compliance review to dynamic behavioral supervision7).

Existing studies have recognized that AI agents are transforming the operational dynamics of digital markets, with concomitant shifts in the boundaries of platform competition, data control, and algorithmic governance. Nevertheless, the majority of the literature remains platform-centric and has paid insufficient attention to the independent competitive functions of AI agents as "decision intermediaries" and "traffic allocation nodes."

Against this backdrop, the present article takes the changes in competitive structure following AI agents' intervention in e-commerce platforms as its primary research object. It focuses on

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.20588248

the reconstruction of platform governance pathways in the AI agent era, advocating a transition from traditional ex-post liability determination to the governance of operational structures. The analysis seeks to re-delineate the power boundaries among platforms, AI agents, and users, thereby preserving technological innovation while maintaining fair competition in digital markets.

2. CONFLICTS BETWEEN AI AGENTS AND PLATFORM POWER

Throughout the development of the digital economy, market competition has consistently revolved around control of market entry points. From early portal websites to search engines and subsequently to platform economies, the entity that controls users' access to information and commodities has occupied a dominant competitive position. With the development of generative artificial intelligence, this previously stable structure is undergoing fundamental reconfiguration: AI agents are progressively displacing platforms as new information intermediaries and decision nodes, thereby inducing systemic shifts in competitive logic.

2.1 Evolution of Market Entry Points: From Platform Centrality to Algorithmic Intermediation

Under the traditional platform economy model, user consumption decision pathways typically followed a unidirectional structure of user–platform–product. Platforms controlled the sequencing of information presentation through search ranking and recommendation algorithms, thereby exercising de facto authority over traffic allocation.

The rise of AI agents is disrupting this structure. Systems such as Perplexity AI, by aggregating and integrating information from multiple platforms, can directly furnish users with cross-platform comparative results and decision recommendations. Users no longer depend on a single platform for information retrieval and selection. The user decision pathway thus transforms into user–AI agent–multiple platforms, with platforms receding from their role as primary "gateways" to become "invoked resources."

This transformation signifies that the core of market competition is shifting from intra-platform rivalry to contestation over entry-point control. The emergence of AI agents is relocating traffic allocation mechanisms—previously concentrated within platforms—to external technological entities. The advancement of artificial intelligence is altering the economic functions of information intermediation and significantly enhancing its role in resource allocation8)

2.2 Reconstruction of the Legal Attributes of AI Agents: From Tools to Quasi-Market Entities

Within existing legal frameworks, AI systems are generally regarded as auxiliary tools, with the legal consequences of their actions ultimately attributed to their developers or users. However, in contexts where AI agents are deeply involved in market decision-making, this tool-based characterization is insufficient to capture their actual influence.

From a functional evolution perspective, AI agents exhibit a clear three-stage progression: first, as information-processing tools that integrate multi-source data to generate structured content;

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.20588248

second, as decision participants capable of producing recommendation outputs based on model inference; and finally, as traffic allocators whose recommendations influence the visibility of different platforms and products. In this process, AI agents cease to function merely as information conduits and instead participate substantively in market resource allocation.

Chinese scholar Zhang Xinbao has observed that algorithmic systems are transitioning from neutral technologies to institutional forces with governance functions, exerting substantive shaping effects on market behavior9). In this sense, simply classifying AI agents as tools and overlooking their actual competitive impact may result in regulatory misalignment.

Accordingly, this article proposes that AI agents should be understood as "quasi-market entities." Although they do not possess independent legal personality, they have acquired the capacity to influence market competitive structures. This conceptualization does not confer full subject status upon them but provides a theoretical foundation for subsequent analysis of their competitive conduct and regulatory pathways.

2.3 Structural Responses of Platform Power: Recentralization Mechanisms

In response to AI agents' reconfiguration of market entry points, platforms are deploying various structural countermeasures to preserve their established competitive advantages. These responses manifest primarily at three levels.

First, at the technical level, platforms reinforce interface control by restricting API calls, modifying access rules, or blocking automated requests, thereby increasing the costs of AI agent access. Second, at the data level, platforms strengthen exclusive control over data through user agreements and technical measures that limit data scraping and reuse. Third, at the rules level, platforms indirectly obstruct the ecological expansion of AI services through contractual constraints or partnership limitations.

The case of Amazon being accused of restricting AI service access illustrates how platforms, when confronted with decentralizing pressures, tend to employ recentralization strategies to maintain control. This phenomenon aligns with the logic of "platform capitalism" in digital platform studies, whereby platforms continually reinforce control over critical resources to consolidate their market position. From a competitive structure perspective, the tension between decentralization and recentralization constitutes a fundamental dynamic of market competition in the AI era. On the one hand, AI agents weaken platforms' gatekeeping advantages through technological means; on the other, platforms reconstruct control boundaries via institutional and technical instruments. The resulting interplay between the two transforms market operations from stable structures into processes of dynamic adjustment.

3. PRACTICAL ISSUES: COMPETITIVE IMBALANCE UNDER THE IMPACT OF AI AGENTS

3.1 Conflicts over Entry Control

In e-commerce platform ecosystems, traffic entrances determine the allocation of information and the pathways of transaction conversion. Traditional models rely on platforms' internal

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.20588248

search and recommendation mechanisms to match users with goods, thereby enabling platforms to retain pivotal control. Upon the entry of AI agents exemplified by Perplexity AI, users may obtain direct product screening and decision-making recommendations through cross-platform information integration, thereby diminishing platforms' central position in the information chain and precipitating an outward shift in entry control.

To preserve their existing advantages, platforms have adopted multiple restrictive measures, including tightening API calls, blocking automated access, revising interface protocols, and constraining third-party AI functionalities through contractual arrangements. Disputes surrounding Amazon illustrate platforms' defensive responses to AI-driven reconfiguration of access points. Although such conduct may be characterised as measures for system security or commercial strategy, the outcome may elevate entry barriers and impair potential competition.

Controversy centres on the legal attributes of interfaces and data channels. Where such resources are indispensable, their control may exert a material influence on market structure. Recent scholarship observes that interfaces and data-access pathways of digital platforms exhibit infrastructural characteristics and should fall within the purview of fair-access regulation 10). Existing rules lack explicit standards for these issues, thereby engendering legal uncertainty.

3.2 Conflicts over Data Control and Institutional Tensions with Personal Information Protection

The operation of AI agents depends heavily on the integration of product information, user reviews and behavioural data, whereas platforms reinforce data control through anti-crawling mechanisms, access restrictions and user agreements, thereby erecting significant data-related competitive barriers. To deliver personalised recommendations and decision support, AI agents frequently require further aggregation of user preference data, including search histories, consumption patterns and behavioural trajectories, in order to construct granular user profiles.

Nevertheless, current legislation has established clear boundaries for the processing of personal information. The Civil Code of the People's Republic of China imposes, in addition to the principles of legality, legitimacy and necessity, a requirement that processing shall not be excessive. The Personal Information Protection Law of the People's Republic of China further introduces the principle of good faith and stipulates that personal information processing must pursue explicit and reasonable purposes, be limited to the minimum scope necessary to achieve those purposes, and refrain from excessive collection or expanded use. The Law adopts a broad definition of personal information, encompassing any information capable of association with a specific natural person.

Against this backdrop, the extensive behavioural and preference data relied upon by AI agents in cross-platform integration may constitute objects subject to legal regulation, thereby subjecting them to dual institutional constraints: technological functionality necessitates deep data mining, while legal norms emphasise "minimum necessity" and "purpose limitation." In the absence of clearly delineated boundaries, data-use practices readily drift between lawful utilisation and excessive processing. The core of the issue therefore lies in the structural tension

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.20588248

between the competitive-resource function of data and its status as a protected right, juxtaposing AI-driven data logic against personal-information-protection principles.

3.3 Distortion of Decision-Making Competition under Algorithmic Dominance

As AI agents become directly involved in user decision-making, market competition is progressively shifting from intra-platform ranking contests to competition among algorithmic recommendations. AI systems determine the scope and priority of information users encounter through screening, ranking and integration, thereby exerting decisive influence on consumption choices. This process, however, typically lacks transparency, rendering it difficult for users to comprehend the generative logic of recommendations or to detect commercial interference or interest-driven bias.

Platforms' own recommendation algorithms may further impose implicit restrictions on external AI services by adjusting ranking parameters, thereby complicating the competitive landscape. Algorithmic opacity may emerge as a new source of market power; competition no longer unfolds through observable metrics such as price or quality but migrates toward invisible strategic interactions within algorithmic systems. Consequently, the transparency and supervisability of market competition are substantially diminished.

3.4 Failure of the Liability Regime

The introduction of AI agents transforms the traditional transaction structure dominated by a single actor into a multi-party configuration comprising "platform, AI agent and merchant." When users suffer harm following decisions made on the basis of AI recommendations, the attribution of liability becomes particularly intricate. Current law neither clarifies whether erroneous AI recommendations constitute legal liability nor delineates the scope of platform responsibility arising from the utilisation of its data by AI systems; similarly, whether merchant liability is altered by AI intermediation remains contentious.

This multi-actor structure renders liability boundaries ambiguous and thereby weakens the efficacy of legal regulation. In the absence of explicit rules for allocating responsibility, parties may exploit structural arrangements to evade liability, undermining the stability of market order. The essence of the problem is that the intervention of AI as a technological intermediary severs the traditional correspondence between conduct and responsibility, producing a structural rupture in the liability regime.

4. INSTITUTIONAL RESPONSES: RECONSTRUCTING REGULATORY PATHWAYS

Following the integration of AI agents into e-commerce ecosystems, market operations no longer depend on a single platform. Information retrieval, product comparison and decision outputs are subsumed within algorithmic architectures, thereby eroding the competitive advantages that traditional platforms derived from entry control and data monopolisation. Existing legal rules, predominantly centred on market dominance, lack effective mechanisms for identifying technologically imposed restrictions, differentiated interface configurations and

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.20588248

algorithmic influence. Regulatory emphasis must accordingly shift towards the operational structure itself, embedding institutional mechanisms that alter the genesis of competitive conduct and thereby render exclusionary practices technically unsustainable.

4.1 Auditable Interface Access

Interface access must operate under a framework of rule primacy, parameter standardisation and process traceability. Foundational information interfaces shall employ standardised open protocols, ensuring uniformity in returned fields, update intervals and invocation ceilings so as to prevent degradation of usability through non-structured responses. Transaction-support interfaces shall adopt tiered access: upon completion of real-name registration and purpose declaration, entities enter a whitelist; differential quota tiers are allocated according to historical compliance records and invocation stability; high-frequency invocations require dynamic quota review, with adjustments grounded in objective metrics such as error rates, anomalous request ratios and contributions to system load. All entities within the same tier are subject to identical parameters; no implicit thresholds may be imposed on the basis of entity type or commercial relationship.

Access controls must be accompanied by auditable logs. Log content shall encompass request-source identifiers, interface type, timestamp, return status, rate-limiting parameters and the criteria for anomaly determination. Rule changes must generate version records specifying the rationale for modification, scope of application and effective date. Regulatory authorities may identify differentiated treatment through sampling comparisons of logs against actual return results. Soft restrictions, such as delayed responses or selective omission of fields, shall be detected by benchmarking response metrics across different entities within identical time windows.

The application of security restrictions must satisfy principles of proportionality and retraceability. Upon detecting attack signatures, platforms may initiate temporary rate limiting or blocking, yet must simultaneously generate an incident report detailing the triggering rule, scope of impact and conditions for lifting the restriction. Measures persisting beyond a reasonable protective period or repeatedly triggered solely against entities possessing competitive functionalities shall be deemed restrictions exceeding security purposes. For emergency measures concerning system stability, ex-post recording is permissible, provided complete logs and explanations are furnished within a prescribed timeframe; otherwise, such measures lack justification.

4.2 Establishing a Behavioural Data Authorisation Pool

The authorisation pool shall function through layered data classification, purpose-bound access and continuous auditing. Data are categorised according to risk and function into public behavioural data, restricted behavioural data and sensitive data. Public behavioural data, after de-identification, enter the foundational pool, encompassing product browsing, click frequency and non-individualised evaluations. Restricted behavioural data, involving preference trajectories and interaction sequences, shall be made available only within explicitly defined purposes and the minimum necessary scope. Sensitive data, comprising identifiable personal

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.20588248

information or trade secrets, are excluded from the general pool and processed exclusively via dedicated authorisation channels.

Access employs dual verification. Entities must submit statements of purpose, model typology and data-processing procedures; access tokens are granted following automated rule checks and manual review. Tokens are bound to specified purposes and temporal windows and become void upon exceeding their scope. Data invocations must carry purpose tags, enabling real-time system matching of purpose and data type to prevent cross-purpose expansion. Invocation records are logged in a unified auditing system, documenting data category, invocation frequency, processing outcomes and deletion nodes.

A "feedback and correction" mechanism is incorporated. Data providers may request review of anomalous invocations, while users may query, through a central portal, the categories and purposes of data accessed concerning them and may exercise rights to restrict or revoke such access. Withdrawn data must be deleted or irreversibly processed within a prescribed period, with destruction records entered in the logs.

Constraints on platforms are manifested through equal-condition supply and quality consistency. Data types employed by platforms for their own recommendation or analytical functions must be made available to external entities under equivalent conditions; platforms may not impair external usage efficacy through reduced precision, delayed updates or sampling bias. Data involving trade secrets or undisclosed transaction information may be placed on exclusion lists, yet categories must be clearly delineated and subject to regulatory filing. Data exhibiting strong substitutability may not be wholly withheld on protective grounds.

Operational compliance centres on continuous auditing. Regulatory authorities identify interface-access or data-restriction violations through cross-comparison of interface logs and data-invocation records; anomalous patterns trigger in-depth examination, with requirements for model-processing explanations where necessary. This mechanism establishes stable boundaries between rights protection and factor circulation.

4.3 Embedding an Influence-Marking Mechanism in Recommendations

AI agents and platform algorithms jointly participate in information distribution, with recommended results occupying a central position in user decision-making. Algorithmic operations remain opaque over extended periods, rendering recommendation logic, commercial interventions and data provenance difficult to distinguish; consequently, competitive processes progressively migrate into unobservable domains. Although the market superficially exhibits multi-party competition, its actual operation may be dominated by a limited number of algorithmic structures. Algorithmic governance therefore requires the conversion of "influence" into identifiable objects. An influence-marking system shall be embedded within recommendation outcomes, decomposing algorithmic functions into three categories: information-structuring, ranking-oriented and decision-substituting. Information-structuring recommendations merely present data in a structured format; ranking-oriented recommendations redistribute users' attention; and decision-substituting recommendations directly generate selection conclusions, thereby exerting substantive effects on user conduct.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.20588248

Each recommendation result must simultaneously display its influence-source structure, encompassing the proportion of data sources, commercial affiliations and the degree of algorithmic participation. Content involving commercial cooperation shall be independently labelled and presented distinctly from organic recommendations. The system shall record the weight variations of each category of influence for subsequent review and comparative analysis. Regulatory authorities may establish differentiated rules according to the intensity of influence, imposing higher disclosure standards and inspection frequencies on decision-substituting recommendations. Algorithmic conduct of platforms and AI agents is thereby transformed into quantifiable indicators, shifting the competitive process from "black-box operation" to observable forms. The space for covert manipulation is compressed, while users are enabled to identify the sources of influence underlying recommendation outcomes.

4.4 Establishing a Segmented Liability Framework along the Decision Chain

Liability at the data-generation stage centres on the authenticity, completeness and legality of input information and is borne primarily by data providers, principally e-commerce platforms or merchants operating on the platforms. The core operations in this stage comprise the collection, verification and output of raw data, including product details, prices, inventory and user reviews. Data providers must institute internal data-validation mechanisms, encompassing real-time inventory synchronisation, cross-verification of multi-source reviews and filtering algorithms for false information, thereby ensuring that interface data disclosed to AI agents contain no systematic distortion or intentional omission. Where subsequent harm is technically traced to inaccurate inputs at the data-generation stage, the data provider shall bear primary compensatory liability and may seek recourse against responsible merchants through platform penalty mechanisms. This stage emphasises "source-level gatekeeping" to compel platforms to enhance their data-governance capacity.

Liability at the recommendation-decision stage focuses on the rationality and compliance of algorithmic screening, weight allocation, personalised integration and final recommendation outputs, and is assumed independently by the AI-agent operator. The operational flow includes feature extraction following multi-platform data scraping, model inference, commercial-interest filtering, user-preference matching and recommendation generation. AI agents must incorporate mandatory explainability modules that record, in real time, the critical decision nodes of each recommendation: the data subset employed, model version, weight-adjustment parameters, exclusion or prioritisation logic and confidence scores. Where algorithmic outputs exhibit significant deviation—such as recommendations generated from outdated data, undisclosed sponsorship relationships or hallucinatory erroneous suggestions—and such deviation bears a causal nexus with user harm, the AI-agent operator shall bear direct liability commensurate with its technical control capacity. AI agents are required to adopt "decision-snapshot" technology, automatically generating cryptographically hashed records upon the creation of each significant recommendation11) and storing them on a neutral third-party audit chain to facilitate tamper-proof ex-post traceability. Liability at the transaction-execution stage corresponds to performance and result assurance subsequent to contract formation and is ultimately borne by the actual merchant. This stage encompasses order confirmation, logistics

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.20588248

arrangement, product delivery and after-sales service. Merchants may not disclaim responsibility on the ground that "the AI recommendation is unrelated to them"; obligations concerning quality guarantees, delivery timeliness and remedies for defects remain unchanged. Where harm occurs during delivery or after-sales processes, liability is directly attributed to the merchant.

This segmented liability framework along the decision chain converts the traditional model, reliant on ex-post oral evidence and subjective inference, into a technical pathway enabling direct attribution based on objective, machine-verifiable records. The liability boundaries among platforms, AI agents and merchants are thereby clearly delineated: data providers govern "source authenticity," AI agents govern "intermediary rationality," and merchants govern "outcome realisation." Regulatory capacity shifts from reactive, case-by-case attribution to proactive structural governance. Through segmented liability and technological embedding, the e-commerce liability system in the AI-agent era is reconstructed into an observable, measurable and accountable dynamic framework, furnishing a solid institutional foundation for a fair order in digital markets.

5. CONCLUSION

Upon the integration of AI agents into e-commerce systems, information retrieval, product filtering and consumption decisions are progressively consolidated within unified algorithmic structures. The competitive advantages previously enjoyed by platforms—derived from entry control, data aggregation and ranking recommendations—are consequently attenuated, while the operational centre of the market shifts toward cross-platform information integration and intelligent decision output. In response to these developments, competitive conflicts manifest principally as structural problems, including entry restrictions, data barriers, algorithmic influence and fractured liability, reflecting the reallocation of traditional platform power structures through technological intermediation.

Addressing these changes requires a regulatory transition from logic centred on single-act adjudication to institutional design oriented toward systemic structures. At the entry level, interface classification and auditing mechanisms constrain platforms' selective restrictions on AI access, thereby reducing the scope for technological exclusion. At the data level, unified authorisation pools and tiered usage rules reconfigure data-control structures, enhancing data circulation efficiency while safeguarding personal-information security. At the algorithmic level, influence-marking and commercial-affiliation disclosure mechanisms increase the recognisability of recommendation processes, compressing the space for covert manipulation. Within the liability system, segmented attribution along the decision chain and traceable recording mechanisms reintegrate multi-party transactional structures into a coherent liability framework.

In summary, AI agents propel competitive rules from a platform-centric structure toward a distributed collaborative architecture, yielding efficiency gains while simultaneously generating novel risks of unfair competition. The crux of institutional response lies not in constraining technological development, but in re-establishing boundary relationships among

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.20588248

entry, data and decision-making, thereby restoring transparency and controllability to market competition and achieving a dynamic equilibrium between technological innovation and a fair competitive order.

Acknowledgments

Though this chapter of my academic journey draws to a close, the path of learning stretches endlessly ahead. As the ancient saying goes, “Those who drink its stream have its source; those who learn its lessons hold their teachers dear.” I would like to express my deepest gratitude to every person who has walked with me along this way.

To Professor Lee, thank you for lighting the lamp of curiosity in my heart, for turning complex knowledge into warm guidance, and for never letting me feel alone in my confusion. Your patience and wisdom have shaped not only how I think, but also how I see the world.

To all who love me and whom I love, thank you for sharing late-night study sessions, silly laughter, quiet days, and all the small, precious moments that make life feel like home. Your presence is my greatest comfort and courage.

And to myself, thank you for never giving up, for choosing to keep going even when things felt hard, and for always staying curious and kind. I am proud of the person I am becoming, and I will keep learning, growing, and walking forward with gratitude.

This is not an end, but a gentle pause before the next step. I will carry all these kindnesses with me, as I continue to grow.

Declaration of Interest Statement

The authors report there are no competing interests to declare.

Funded research project

This research is supported by the Research Project of the Ministry of Justice on Rule-of-Law Construction and Legal Theory, entitled “Research on the Optimization and Governance Strategies of the Intellectual Property Ecosystem Empowered by Blockchain Technology” (Grant No. 22SFB5044).

References

1) Scott Morton, F. (2023). Equitable interoperability: The “fair access” approach to regulating digital platforms [J]. Journal of Competition Law & Economics, 19(2):1-35.

2) Calo, R. (2023). Artificial intelligence policy: A primer and roadmap [J]. University of Chicago Law Review, 90(1):1-45.

3) Veale, M. (2024). Demystifying the draft EU Artificial Intelligence Act [J]. Computer Law Review International, 25(1):1-15.

4) Floridi, L. (2025). AI governance, digital power and the future of regulation [J]. Philosophy & Technology, 38(2):1-18.

5) 张新宝.个人信息保护法的体系结构与基本制度[J].中国法学, 2021(04):5-20.

6) 高富平.数据要素流通中的权利配置与制度协调[J].法学研究, 2024, 46(03):22-39.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.20588248

7) 丁晓东.生成式人工智能的算法治理与法律回应[J].现代法学, 2025, 47(02):118-132.

8) Varian, H. R. (2019). Artificial intelligence, economics, and industrial organization. In The economics of artificial intelligence: An agenda (pp. 399–419). University of Chicago Press.

9) 张新宝. (2021). 个人信息保护法的体系结构与基本制度. 中国法学, (4), 5–20

10) Scott Morton, F., et al. (2023). Equitable interoperability: The “fair access” approach to regulating digital platforms. Journal of Competition Law & Economics, 19(2), 1–35.

11) Synthetic Data News. (2026). AI Decision Logging Specification: Open specification for tamper-evident AI decision logs [GitHub Repository].