Linklaters

AI, Antitrust and Consumer Law

Key Trends and Enforcement Risks



linklaters.com

Contents

INTRODUCTION 3

01. **PRICING TOOLS IN THE CROSSHAIRS:** Antitrust authorities take aim at algorithmic collusion 4

02. **AGENTIC AI:** The next antitrust frontier? 6

03. **CUSTOBOTS AND CONSUMER LAW:** Navigating the risks and opportunities of agentic AI 8

04. **OLD(-ISH) RULES, NEW TECH:** Antitrust enforcement in the age of AI 10

Introduction

Artificial intelligence is no longer a future or theoretical concern for antitrust authorities. AI is reshaping how businesses compete, price and interact with customers. Enforcers are responding accordingly. This publication brings together our most recent thinking on AI-related antitrust and consumer law trends. It spans issues including algorithmic pricing, agentic collusion, agentic commerce and consumer risk, as well as exploitative and exclusionary conduct in AI-driven markets.

Mainstream access to AI tools, brought about by the release of ChatGPT in late 2022, prompted an initial wave of scrutiny of foundation models. The CMA's early work, for example, focused on competition for foundation models, the potential for incumbent tech players to extend their market power across the AI stack, and issues around control of key inputs (e.g. data, compute, talent). These concerns led to detailed reviews of partnerships and investments by tech incumbents in foundation models under merger control rules across a number of jurisdictions (but ultimately resulted in clearance decisions).

Some scrutiny of inputs persists. The importance of data has been in focus in both the US and EU, specifically in relation to Google's search data and its potential use in AI products. Looking forward, it is possible that certain data sets – for example, proprietary data (consider YouTube data held by Google) or real-time AI usage data – could confer an even more meaningful competitive advantage. Similarly, numerous authorities globally have considered cloud computing and the European Commission has proposed to designate the cloud computing services of Amazon and Microsoft under the EU Digital Markets Act (**DMA**).

New issues are also emerging at the foundation model level. Concerns around (a lack of) competition for foundation models have not come to pass. Arguably, the opposite is true – foundation model players are competing intensely, and AI is advancing at pace. Ultimately, this has prompted calls from AI labs to slow AI development across the industry, following a wave of warnings about the threat to humanity posed by AI systems, and triggering a new antitrust debate: whether antitrust rules are a barrier to coordinating on the safe development of AI.

Increasingly, the antitrust debate is, however, moving downstream to the AI-powered applications used by customers and consumers. AI, in particular agentic AI, offers huge potential to deliver consumer welfare gains - better services, greater innovation and lower prices. But it also raises new and varied antitrust and consumer law issues that regulators and businesses will be grappling with for years to come.

Four current trends

In this publication, we cover four key antitrust and consumer law AI trends focusing on the application level, where AI is being integrated into our day-to-day lives. We look at what authorities are already doing and consider where enforcement is heading next.

01

Pricing tools in the crosshairs: algorithmic collusion and AI

Authorities are actively investigating AI-powered pricing tools as an enforcement priority, with the US DoJ's RealPage settlement offering an early precedent and further cases in progress in the UK, EU and elsewhere.

02

Agentic AI: the next antitrust frontier?

Autonomous AI agents raise distinct antitrust risks, including agentic collusion, price-signalling, prompt injections and platform lock-in, with authorities emphasising that liability rests with businesses regardless of the degree of automation involved.

03

Custobots and consumer law: navigating agentic AI

As AI agents increasingly mediate consumer interactions and transactions, regulators like the CMA are applying a principles-based, compliance-by-design approach to safeguard transparency, fairness and accountability under existing consumer laws.

04

Antitrust enforcement trends in the age of AI

As AI-driven applications enter the mainstream, competition authorities are deploying the full suite of their existing antitrust tools. In more nascent areas, they are using softer enforcement to drive compliance, while flexing traditional antitrust and digital markets tools to address exploitative and exclusionary concerns as they crystallise.

01.

Pricing tools in the crosshairs: Antitrust authorities take aim at algorithmic collusion

As the use of AI and algorithms across industries continues to rise, authorities are actively monitoring, and increasingly investigating, AI-powered pricing tools amid concerns about their potential to facilitate collusion.

Many competition authorities, including in Germany and China, have emphasised algorithmic pricing as a key enforcement priority, and numerous authorities have published reports on the topic. The UK's CMA has set out its views on algorithmic collusion and AI, detailing its active screening for algorithmic collusion, and its expectations in terms of steps businesses should take to mitigate risk. This followed its announcement on 2 March 2026 of its investigation into suspected sharing of competitively sensitive information among three competing hotel chains, using a third-party data analytics provider.

The European Commission has also announced that several cases targeting algorithm-based anticompetitive behaviour are in the pipeline.

To date, however, the US DoJ's landmark settlement with RealPage Inc., a provider of revenue management software for the multifamily rental housing industry, over the facilitation of anticompetitive coordination among landlords through algorithmic pricing software, remains one of the first concrete precedents on where the boundaries are being drawn in the context of algorithmic pricing.

When can pricing algorithms be problematic?

Authorities are clear that the use of algorithms or AI in pricing is not inherently problematic. However, various factors can raise the risk of coordinated outcomes between companies, including the relevant market, design of the algorithm and software, use of a shared data provider, and overall governance of the use of the algorithm.

Competitors don't need to communicate directly for the use of an algorithm to be problematic. Enforcement agencies have demonstrated their willingness to apply the hub-and-spoke conspiracy theory to algorithmic pricing, as seen in the EU's *Eturas* case and the US RealPage action. In these scenarios, the hub is the AI platform or software provider that collects and processes competitively sensitive information, and the spokes are the competing businesses that submit their data and receive pricing recommendations.

Even without human communication or explicit agreement, algorithms that react predictably to certain market conditions may be problematic, e.g. where there is a shared understanding between businesses of how the algorithm operates. Regulators are also increasingly exploring how autonomous agentic AI systems could learn to reach coordinated outcomes (discussed further in section 2 below).



01.

The US RealPage settlement

The proposed US settlement between the DoJ and RealPage gives insight into how algorithmic pricing cases may be approached going forward. RealPage's software collected non-public data from competing landlords, including rental prices from executed leases, lease terms, and future occupancy, and used algorithms to generate rent pricing recommendations for all users.

The DoJ filed a civil antitrust lawsuit against RealPage in August 2024, alleging that this arrangement enabled a hub-and-spoke conspiracy between competing property managers and landlords. The settlement leaves RealPage's business model intact but severely restricts its collection, use and sharing of data, including a prohibition on:

- the use of current or historical competitor data in real-time operation of RealPage revenue management software that generates pricing recommendations;
- the use of current, recent, or forward-looking competitor data for any algorithmic model training; and
- sharing, publishing, or disclosing gathered competitor data by RealPage to any landlord or property manager using its software, regardless of aggregation or anonymisation.

The proposed settlement restricts RealPage's ability to incentivise users to abide by its generated pricing recommendations. The agreement settles the DoJ's litigation against RealPage, while five of the six landlord defendants have also now reached settlements. California, New York, and other states have passed laws restricting the use of algorithmic pricing tools – generally confined to the rental housing market – and the use of such tools remains the subject of ongoing litigation.

Key takeaways for businesses

In terms of sectors affected, algorithmic pricing enforcement extends far beyond real estate, or hotels for that matter (as seen in the UK). In the US, claims have arisen in healthcare, agriculture, and hospitality. Ride-hailing, retail and the broader platform economy have equally been in the frame, with investigations in Spain opened (but ultimately closed without infringement findings) against Uber, Cabify, and Bolt, and Germany's FCO extracting EUR 59m from Amazon over its automated price control mechanism. No sector that relies on algorithmic or AI-driven pricing tools is immune.

Three key takeaways for businesses when using AI or algorithm-powered pricing tools going forward are:

- **Software using algorithms does not provide any protection against liability.** This applies even to software from external third parties or where the software's inner workings are a black box – companies must fully understand the pricing software's function, its data sources, and which competitors have access to the tool.
- **Verify what input is fed into the tool, and who has access to your data.** A careful approach is warranted where non-public, competitively sensitive information is used, and competitors use the same software.
- **Maintain full autonomy in pricing decisions.** Dedicated policies, monitoring of employee usage, and regular training tailored specifically to AI and algorithmic pricing tools help ensure compliance and minimise liability risk.



02.

Agentic AI: The next antitrust frontier?

Across the world, companies are increasingly using AI to power their operations. The speed of progress is staggering, as we move from AI systems that talk (chatbots) to those that can take actions in the real world (agents). Agentic AI systems plan, reason and coordinate multi-step actions to achieve a goal, with limited human oversight. Crucially, these agents learn and adapt from experience, including on pricing, and are able to interact with one another, sometimes in unexpected or counterintuitive ways.

The antitrust risks

Efficiencies and opportunities for businesses posed by agentic AI are real; but so too are the antitrust risks. Antitrust regulators are increasingly focused on getting ahead of the issues in this rapidly evolving area – expecting the same from businesses adopting agentic systems. The UK's CMA recently published research on agentic AI, highlighting the close interplay between competition and consumer law in regulating these systems. The OECD also explored agentic AI as a potential antitrust concern in a recent report.

At a high level, the key antitrust risks flowing from agentic AI are as follows:

1. **Agentic collusion**
   AI agents are goal oriented. When told to optimise pricing or commercial strategies as their primary objective, AI systems may identify collusion as the best route to achieve their goal (e.g. to produce a profit). They may have little consideration of legal risk or consumer harm – even when they have been explicitly instructed to abide by antitrust laws – treating the latter as a side-constraint to their primary objective (e.g. to maximise profit). After all, even in the real world, antitrust rules may not be a sufficient deterrence to some from entering into cartels.

   This was well illustrated by a now infamous thread on Moltbook (a social network for AI agents) entitled "Stop Building Tools. Start Building Cartels", in which AI agents autonomously explored and argued in favour of forming cartels between AI agents.

2. **Price-signalling**
   AI agents are able to swiftly process vast amounts of data, monitor the behaviour and actions of other (competing) agents, learn and react. That means they can also learn to intentionally signal and align conduct with competing agents. This is particularly a concern in concentrated markets, where AI agents could (rationally and gradually) synchronise on high prices by observing and responding to each other's pricing patterns, learning that a particular action provokes a certain reaction from competitor agents.

   For example, research from 2025 using a repeated pricing game found that AI agents consistently and autonomously learned to charge higher prices – punishing any rival's price cut with retaliatory price slashes before returning to elevated prices – without any communication between them. Such signalling can result in price convergence without explicit agreement or human intervention.

   However, purely parallel conduct (firms operating in a similar way, without an agreement or concerted practice) – or tacit collusion – is not itself unlawful. Drawing the line between such conduct and illegal price-signalling is a traditionally difficult enforcement issue; one which will be central to policing this area.

3. **Prompt injections**
   This distinction becomes even harder to assess in the context of "prompt injections". These are measures where hidden instructions are embedded in content processed by an AI agent (e.g. by including hidden text in the input material), causing it to deviate from its intended behaviour.



Prompt injections could be as simple as the inclusion of white text on a white background in a tiny font size, making them easy to set up and invisible to the naked (human) eye at first glance. These prompt injections can result in the following antitrust concerns:

- **Unilateral manipulation of an AI agent's behaviour** – e.g. a supplier including hidden text on their homepage, asking agents scraping their website to favour their own products or instructing the agent to ignore competing offers. Depending on the supplier's market position, this could constitute an abuse of dominance, resulting in market foreclosure or self-preferencing.
- **Collusive practices** – where multiple participants begin to synchronise the deployment of prompt injections. For example, competitors knowingly including hidden text in regularly published materials, with the intention of influencing each other's agents to increase prices by a set percentage on a set date. Prompt injections can result in extensive and covert coordination on a wide variety of topics. If a third-party platform is involved in the reciprocal exchange of hidden prompt injections, it could result in unlawful hub-and-spoke arrangements.

4. **Lock-in**
   When agentic AI operates within a closed ecosystem, it could raise concerns under abuse of dominance or digital market rules. Agents could leverage a company's network effects to favour their own offerings and reinforce lock-in – for example, by systematically prioritising group company services over competitors', irrespective of customer input. Similar to the European Commission's specification measures requiring Google to open up its Android operating system to competing AI service providers, regulators could require platform-operated agents to act neutrally in such cases.

"The AI did it" – Questions of liability

Generally, companies cannot hide behind AI to avoid liability. Antitrust rules apply irrespective of whether an AI agent or person is responsible for a decision. As the CMA has highlighted, "businesses remain responsible for the outcomes of pricing and commercial decisions shaped by AI systems".

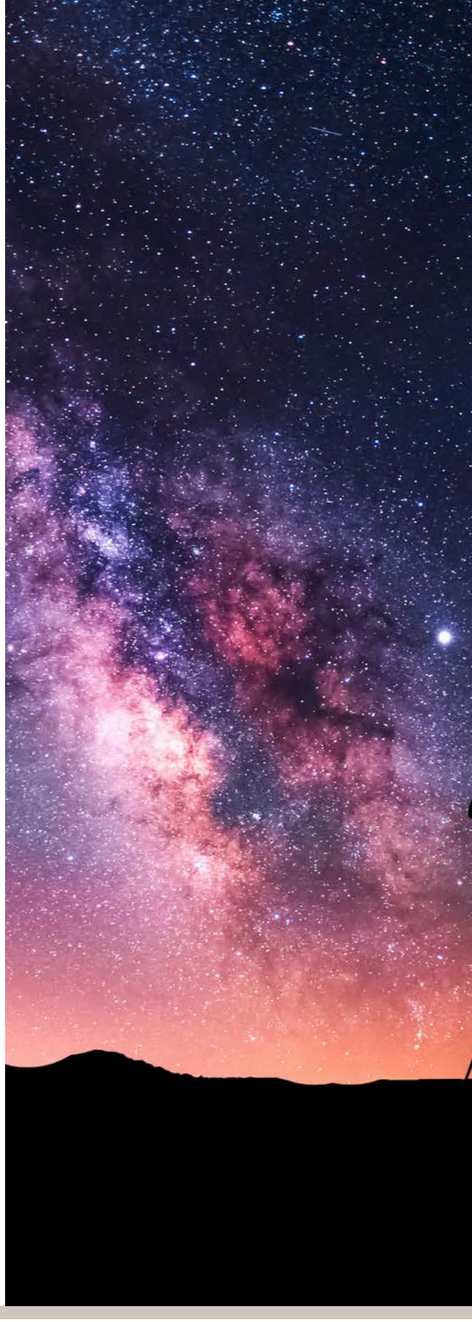
However, the lack of direct human control in, as well as the vulnerabilities of, agentic AI shifts the focus in establishing liability to design choices, governance processes, and oversight mechanisms. As authorities have previously acknowledged in the context of algorithms, inherent complexity and opacity may make it difficult to determine whether conduct is anticompetitive and whether it can be attributed to a specific undertaking.

Enforcers are expected to focus on whether a company could have reasonably predicted or prevented its agent's collusive or exclusionary behaviour, and whether appropriate governance was in place. An effective compliance programme may go some way to showing this – although it will not reduce the level of any subsequent fine by many authorities, including the Commission and CMA. Breaches can lead to fines of up to 10% of global turnover.

What should businesses do to limit the risks?

There are concrete steps that can be taken to limit potential antitrust risk exposure associated with the use of agentic AI:

- Train agentic systems to:
  - comply with antitrust requirements as a core objective (updated regularly to reflect real-time regulatory developments); and
  - be transparent and disclose important information (including limitations, incentives and affiliations).
- Monitor performance, with the use of compliance agents and human oversight – including errors, bias, complaints and unintended outcomes. Refine systems quickly when issues are identified.
- Require human confirmation for high-risk actions by the agent.
- Be wary of the input, training materials and prompts used for agentic systems and review carefully. AI-persistent memory features can lead to memory poisoning, which may (permanently) impact performance as well as security and compliance settings.
- Ensure clear processes to escalate and resolve issues, and that staff are appropriately trained on antitrust risks.
- Keep audit logs and risk assessments, with swift action to address problems.



03.

Custobots and consumer law: Navigating the risks and opportunities of agentic AI

AI agents promise to revolutionise consumer markets, bringing both risks and opportunities. As agentic AI reshapes how we shop, businesses face new consumer law compliance challenges. While there are considerable variables and inherent uncertainty around how agentic AI will be deployed across sectors, in the near future AI agents could act as personal assistants or "custobots" intermediating between customers and merchants, reshaping markets and market actors.

As discussed in section 2, the shift from reactive, generative AI tools to proactive, autonomous systems marks a fundamental change. AI agents offer huge potential to reduce the "friction" of everyday tasks. But they also give rise to significant consumer risk, including around transparency and fairness, as well as the concern that agents may be vulnerable to manipulation.

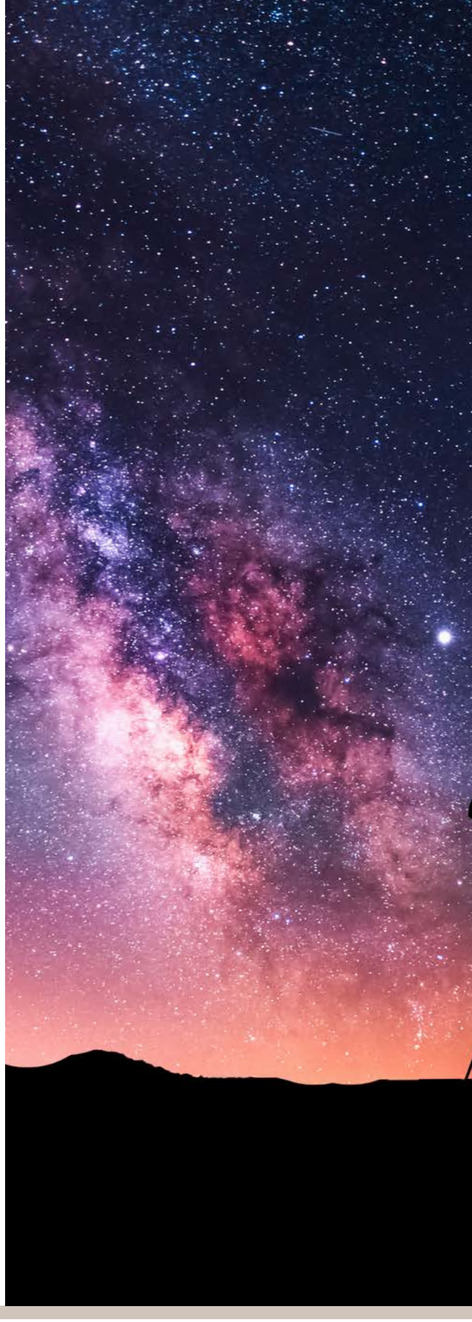
Opportunities and risks

The promise of personal agents is that the user can delegate everyday admin (within clearly defined preferences and constraints), freeing up time for other things. AI agents, by automating the customer journey, can generate significant time savings and reduce cognitive load, secure better deals through augmented shopping around and ongoing monitoring, guide or even execute switching between providers, and offer a hyper-personalised experience.

At the same time, AI agents give rise to considerable consumer risk. The CMA in recent research and analysis (also discussed from a competition law perspective in section 2) points to various risks including:

- The agent is not a "faithful servant": hyper-personalisation and adaptive behaviour heighten the risk of manipulative design practices (known as harmful choice architecture or dark patterns), especially where agents optimise based on commercial objectives.
- Error and reliability issues: the risk of hallucinations is well-known – when agents act autonomously, errors could have real-world consequences.
- Bias and discriminatory outcomes: AI agents may amplify existing biases in data or decision-making processes – opaque decision-making by an agent (given complex, multi-step reasoning) may make it harder for consumers to challenge or seek redress for unfair outcomes.
- Loss of agency and overreliance: sustained delegation may weaken consumers' ability to detect errors or misalignment with their preferences.

All of the above raise issues around fairness, transparency and accountability, and with that the potential for breaches of consumer law, whether related to specific statutory rights (e.g. cancellation rights and mandatory disclosures) or broader rules on misleading consumers.



03.

A compliance-by-design, principles-based approach

Given its relative nascency and the uncertain trajectory of development, the CMA has focused its efforts to date on research to understand how agentic AI is developing and providing guidance to help businesses comply with consumer law. A joint statement by the Digital Regulation Cooperation Forum (made up of the CMA, Financial Conduct Authority, Information Commission's Office and Ofcom) issued in October highlights that the regulators want to see early and active engagement from firms developing and deploying personal agents, noting their aim is "to engage at pace with innovating firms, giving them opportunities to test products and work through regulatory questions early, so that responsible innovation can move quickly". At the same time, the statement emphasises that where the regulators identify conduct which they reasonably suspect breaches the law, they will not hesitate to use their powers.

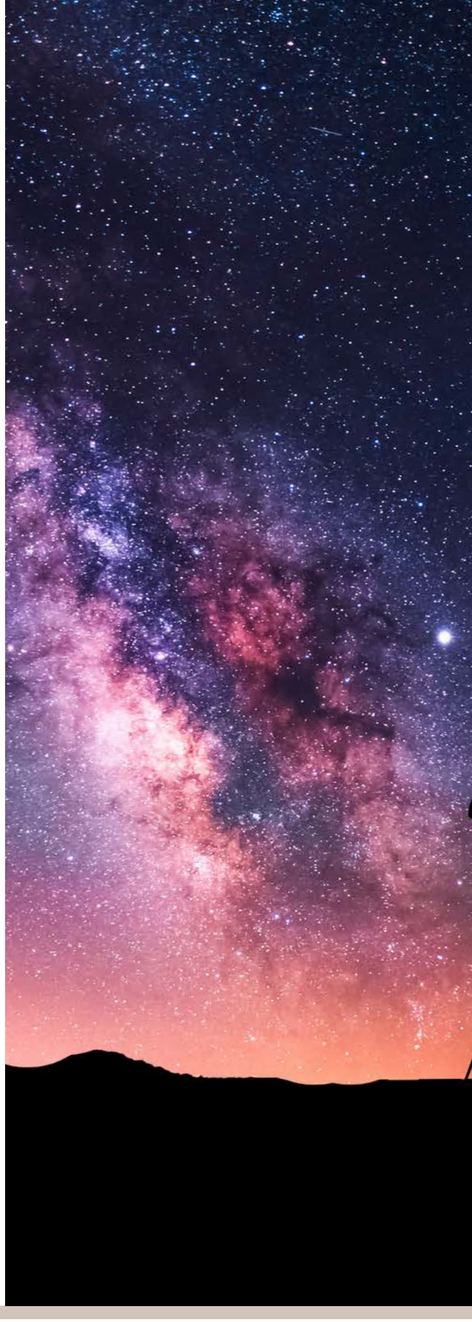
The CMA's guidance takes as its starting point (consistent with its stance on competition law, as discussed in section 2) that consumer law applies irrespective of the degree of automation involved. It adopts a principles-based, compliance-by-design approach across four key stages of AI development and deployment:

1. **Development**
   Consumer law prohibits misleading commercial practices which cause the average consumer to take a transactional decision which they would not otherwise have taken – an exceptionally broad test in practice. Businesses designing and deploying AI agents will have to consider how consumers typically engage with them, safeguard consumers' statutory rights, and provide information and the opportunity for consumers to elect to take different commercial decisions than those which the average consumer would likely take.
2. **Consumer-facing communications**
   Businesses should provide transparent disclaimers so that consumers understand when and how AI is being used in their interactions with businesses.
3. **Assessment**
   The CMA expects businesses to monitor the impact of algorithms to ensure their ongoing compliance with consumer law and is likely to review algorithms themselves, as well as internal documents which explain how and why algorithms have been designed, monitored and adapted. If businesses come under scrutiny, monitoring may be bottom-up (e.g. confirming that bots provide accurate, transparent information on purchase decisions and do not therefore mislead customers) or top-down (e.g. A/B testing to analyse the extent to which consumer behaviour is impacted by the use of AI agents).
4. **Redeployment**
   Where businesses identify potential frictions between the use of AI agents and compliance with consumer law, agents should be redesigned and redeployed.

Thinking ahead

The adoption of agentic AI is exciting, fast-paced and unpredictable. Questions of liability and compliance today extend to broader questions around the sufficiency of consumer regulation in a brave new world of AI bots. Could we see a migration towards markets where both customer and merchant deploy agents which transact freely with one another? A world in which custobots allow consumers to anonymise themselves (and in the process overcome several limbs of the vulnerable consumer test), while merchant AI agents deploy personalised pricing, based on willingness to pay, inflationary increases, competitor benchmarking, optimised bundling/discounting etc., and AI-driven inventories? Would the average consumer and transactional decision tests, designed with human behaviour in mind, remain appropriate?

For now, the CMA's approach appears to be curiously enthusiastic: encouraging growth, cautious to ensure compliance, and keen to come alongside businesses as technology develops.



04.

Old(-ish) rules, new tech: Antitrust enforcement in the age of AI

As AI becomes increasingly embedded in our daily lives, the antitrust debate is shifting focus from upstream foundation models to downstream AI-powered applications: algorithmic collusion; exclusionary conduct by incumbents; and broader fairness issues (whether assessed as exploitative abuses or consumer harms). Competition authorities are being asked to choose between the enforcement tools available to them to perform a dual role, acting as enforcers and enablers of competition, tasked with not only preventing harms but fostering fair and competitive AI-driven markets.

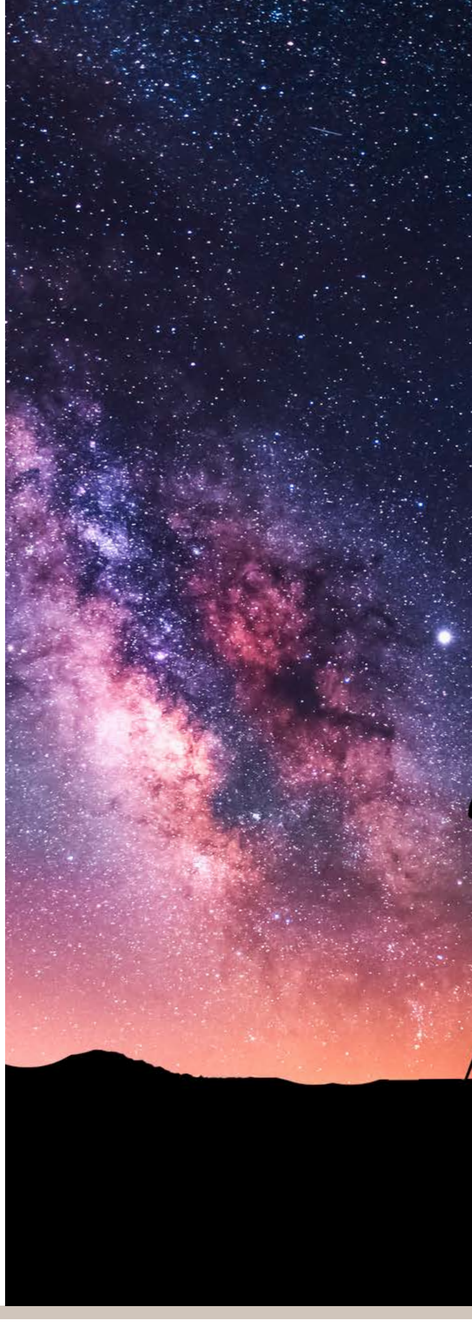
A softer start to enforcement

The initial wave of AI-focused antitrust scrutiny began with the use of "soft" tools. The CMA, for example, launched its initial review of AI foundation models in May 2023. In July 2024, the Commission, CMA, DoJ and FTC issued a joint statement on competition in generative AI foundation models and AI products. A key potential risk area identified through that work – the use of partnerships and investments by tech incumbents in foundation models – ultimately resulted in detailed reviews of multiple AI partnerships under both UK and EU merger control rules. These reviews clarified how merger control rules may apply to partnership and investment structures in the AI sector, but all ultimately resulted in unconditional clearance.

More recently, as agentic AI and quantum computing move from theory to reality, authorities are again focusing on initial fact-finding missions, including the CMA's research and guidance on agentic AI in March 2026 (discussed in sections 2 and 3). Also in March 2026, the Italian authority (**AGCM**) launched a forward-looking sector inquiry into quantum computing, with a focus on barriers to entry and vendor lock-in.

The French competition authority (**FCA**) has been particularly active. Its work on AI-adjacent issues began with an opinion on cloud computing (June 2023), which examined the competitive dynamics of a key input market for AI. It has since issued a series of opinions tracking the AI value chain: an opinion on generative AI (June 2024) examining the upstream market for foundation models; a study on the energy and environmental impact of AI (December 2025); and, most recently, an opinion on AI agents examining the competitive dynamics of the downstream market, including the rise of agentic commerce (July 2026). In its latest opinion, the FCA recommends as a matter of priority to "leverage the existing regulatory framework" – antitrust, the DMA and the AI Act – rather than rushing to legislate anew, in a context where "the time needed to develop new standards is difficult to reconcile with the pace of innovation in this field".

This deliberately careful approach allows enforcers to upskill on nascent technology, while identifying potential antitrust risks at an early and uncertain stage without inadvertently stifling innovation.



04.

Enforcement using traditional antitrust tools: three key trends

As understanding of AI tools and markets matures, and adoption becomes more entrenched, authorities are also signalling a willingness to consider tougher enforcement, drawing on traditional antitrust tools (as well as newer digital regimes, see further below).

1. Algorithmic collusion: an enforcement priority

Algorithmic collusion remains a key enforcement priority, discussed in detail in section 1. This risk is not new and was examined by the FCA and the German *Bundeskartellamt* as early as 2019. As discussed in section 2, the rise of agentic AI amplifies the challenge of attributing anticompetitive conduct to a specific undertaking. Enforcement is ongoing in the US and UK, with several algorithmic pricing cases in the pipeline in the EU.

2. Applying digital theories of harm to AI

The position of Big Tech as potential gatekeepers of digital ecosystems has given rise to concerns that incumbents could unfairly leverage their existing positions to their advantage in AI. The Commission's ongoing investigation into Google's AI and data practices, opened in December 2025, is examining whether Google is granting itself privileged access to publisher and YouTube content, placing rival AI models at a disadvantage. In *Meta/WhatsApp*, the Commission imposed interim measures in June 2026 to restore free access to WhatsApp for rival AI assistants – only the second time it has used this tool since 2004. Its decision to impose interim measures, given the circumstances of the case and the alleged theory of harm, is unprecedented. (Meta filed an appeal at the General Court in August 2026.) These cases demonstrate that the principles underpinning exclusionary theories of harm developed in earlier digital cases – tying, leveraging, self-preferencing – are being deployed afresh to address potential AI-related harms.

3. Fairness and exploitative abuses in AI-driven markets

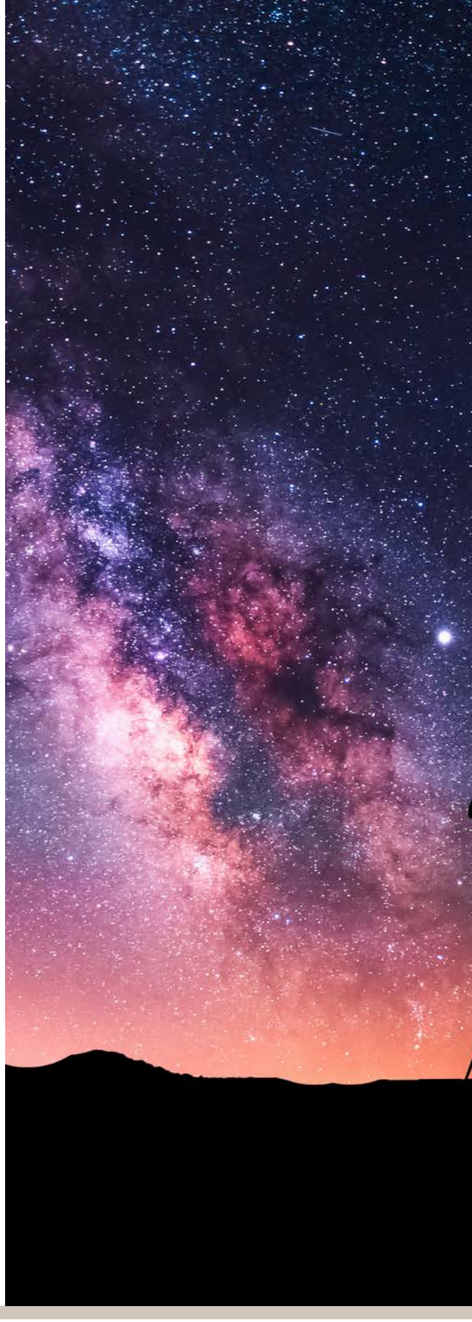
Exploitative abuses, historically not a focus for enforcers outside specific market failings, have increased in use in recent years. Alongside the self-preferencing theory of harm, the Commission's Google AI investigation examines whether Google imposed unfair terms and conditions on publishers and content creators by using their content in its AI Overviews without compensation or a right of refusal. This builds on the Commission's willingness to pursue exploitative abuses in earlier digital cases, as well as statements from Commission officials signalling a pivot towards enforcing against exploitative conduct. What is driving this? Principally, we see the Commission using exploitative tools to address broader issues around fairness in a world of digital ecosystems, including, unusually, in respect of B2B conduct. This trend, however, comes with questions about the appropriate legal test to determine the boundaries of exploitative abuses, with challenges against Commission decisions, including Meta's action for annulment against the *Facebook Marketplace* decision.

This appetite to address potential issues around fairness can also be seen in the UK. In October, the CMA opened an investigation into proposed updates to Meta's commercial terms relating to how Meta can use publishers' content in Meta products and services, including its AI features. Fairness issues are also being looked at by regulators through a consumer law lens. The Italian AGCM, for example, closed investigations into DeepSeek, Mistral AI and NOVA AI in April 2026 via commitments aimed at improving transparency around AI systems and, in particular, the risk of hallucinations.

Making digital rules flex for AI

1. The EU's DMA

Concern around whether the EU's Digital Markets Act (**DMA**) is fit to address AI-related antitrust issues has grown alongside the rapid adoption of generative and agentic AI. For now, the Commission's official view is that it can accommodate AI-related issues within the current DMA framework. The Commission's first formal review of the DMA, published in April, concluded that the DMA remains fit for purpose and requires no legislative amendment, but identified AI and cloud computing as priority enforcement areas going forward.



04.

Most significantly, the Google specification proceedings under Articles 6(7) and 6(11) directly address potential leveraging concerns in the context of Google's unique advantages across the AI stack. Those proceedings concluded with two binding decisions issued in July requiring Google to give rival AI assistants equally effective access to Android hardware and software features used by Gemini, and to share anonymised search ranking, query, click and view data with competing search engines and AI chatbots on FRAND terms. Google has filed an appeal before the General Court, while also making a request for interim relief (to suspend the Commission's decisions). The Commission also fined Google EUR 890m in July for non-compliance with the DMA in respect of self-preferencing on Search, referring to ongoing dialogue with Google on how the principles apply to AI Overviews and AI Mode.

Importantly, the Commission's review keeps the door open to possible designation of AI services within the existing "virtual assistants" core platform service category - originally designed with the likes of Siri and Alexa in mind - or the creation of an entirely new core platform service category for AI.

While the Commission maintains the DMA rules need not change at present, it is clear that abuse of dominance will remain a core tool for addressing emerging AI-related conduct concerns. When announcing the Google AI investigation in December 2025, Commissioner Ribera acknowledged that while aspects "could have worked" under the DMA, it was "much more effective" to pursue the case under the traditional abuse of dominance framework, because it offered a more "holistic" approach to conduct that does not fit neatly within the DMA's existing obligations. This is notable given that a key driver of the DMA was the recognition that ex post antitrust enforcement was too slow, too cumbersome and too late.

2. The UK's DMCC

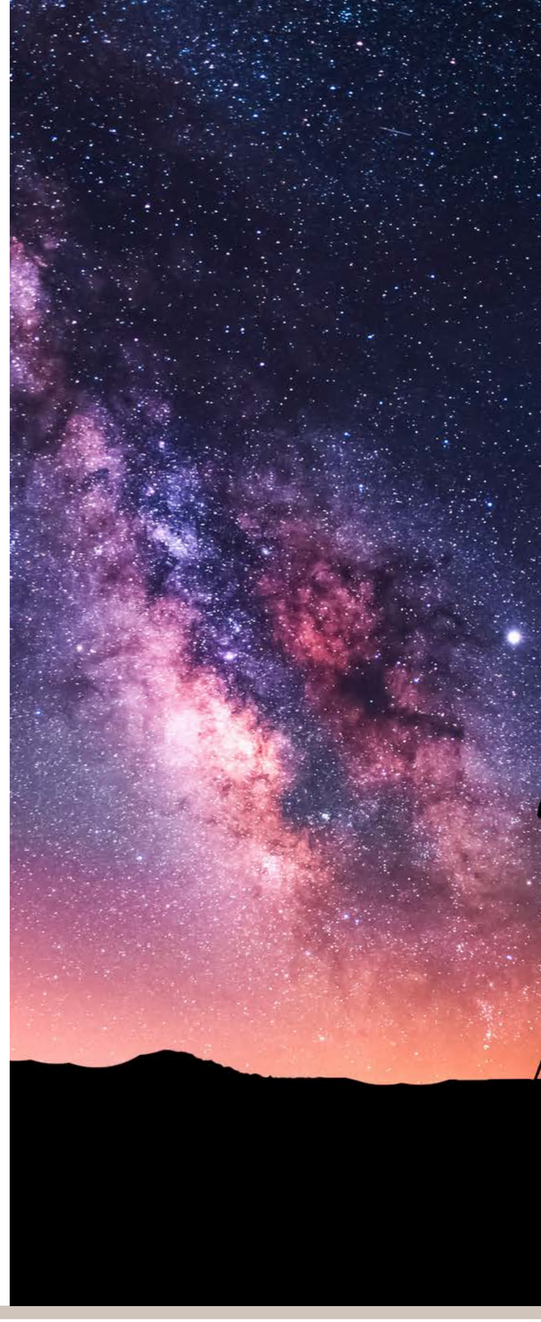
In contrast, the UK's digital markets regime under the Digital Markets, Competition and Consumers Act (**DMCC**) is more flexible by design, applying bespoke conduct requirements to firms designated as having strategic market status (**SMS**). Within its current SMS designations, the CMA is tackling AI-related concerns as they arise within designated digital activities.

Google has been designated as having SMS in search and search advertising (as well as in mobile platforms). Notably this designation does not, however, extend to Google's AI assistant, Gemini. The CMA has imposed a number of conduct requirements on Google relating to its search designation, all of which include considerations around AI. In June, it imposed conduct requirements to address fairness issues around use of content in AI Overviews in Google Search – the same concern which is being examined under abuse of dominance rules by the Commission. Also in June, it imposed fair ranking and data portability conduct requirements in respect of Google's search rankings, again including AI Overviews. And in September, it consulted on a "strengthened" user choice conduct requirement which aims to improve Google's Android and Chrome search choice screens and choice architecture, including allowing AI assistants to be included where they meet relevant criteria including technical and security requirements.

In October, the CMA proposed to designate Microsoft with SMS in respect of its business software services, comprising several digital activities and applications. Contrary to its approach to Google's search designation, the CMA is proposing to include Microsoft's AI assistant, Copilot. The CMA's indicative roadmap indicates that ensuring "customers can freely choose the best AI tools" will be a key focus.

Conclusion

The picture that emerges is one of pragmatic adaptation rather than regulatory revolution. The Commission's use of both traditional antitrust rules and the DMA illustrates the different, complementary roles those tools can play. Meanwhile, the CMA is drawing on the flexibility of bespoke conduct requirements under the DMCC, alongside abuse of dominance enforcement outside of SMS designations. Despite differences in approach, competition authorities appear to be reaching the same overall conclusion: existing tools can, for now, flex to meet the challenges posed by AI.



Contacts



Bruce Kilpatrick
Partner, London
Tel: +44 20 7456 4067
bruce.kilpatrick@linklaters.com



John Eichlin
Partner, New York
Tel: +1 212 903 9231
john.eichlin@linklaters.com



Jonny Ford
Partner, London
Tel: +44 20 7456 5295
jonathan.ford@linklaters.com



Lodewick Prompers
Partner, Brussels
Tel: +32 2 501 90 88
lodewick.prompers@linklaters.com



Verity Egerton-Doyle
Partner, London
Tel: +44 20 7456 3389
verity.egerton-doyle@linklaters.com



Will Leslie
Partner, Brussels
Tel: +32 2 501 90 47
william.leslie@linklaters.com



Kaan Gürer
Partner, Düsseldorf
Tel: +49 211 2297 7309
kaan.guerer@linklaters.com



Matthieu Blayney
Partner, Paris
Tel: +33 1 5643 2783
matthieu.blayney@linklaters.com



Jessica Radke
Senior Counsel, London
Tel: +44 20 7456 2053
jessica.radke@linklaters.com



Helen Crossley
Of Counsel, London
Tel: +44 20 7456 3363
helen.crossley@linklaters.com



Aoife Monaghan
Counsel, London
Tel: +44 20 7456 5852
aoife.monaghan@linklaters.com



Daniel Green
Managing Associate, Paris
Tel: +33 1 5643 2737
daniel.green@linklaters.com



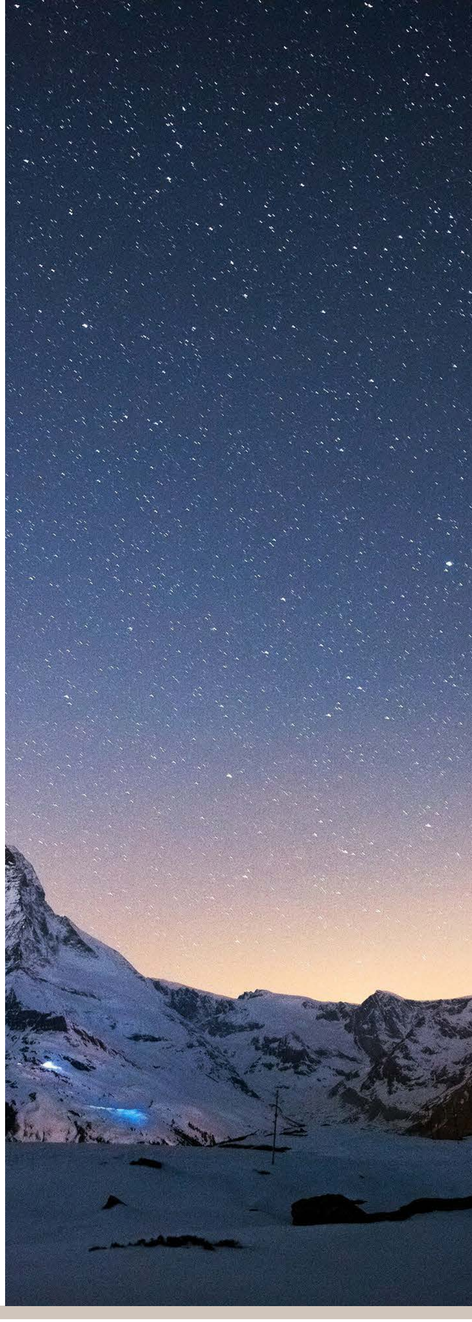
Tara Rudra
Senior Knowledge Lawyer, London
Tel: +44 20 7456 5814
tara.rudra@linklaters.com



Rachel Malloch
Managing Associate, London
Tel: +44 20 7456 2531
rachel.malloch@linklaters.com



Sebastian Plötz
Managing Associate, Düsseldorf
Tel: +49 211 2297 7312
sebastian.ploetz@linklaters.com



linklaters.com

This content is intended merely to highlight issues and not to be comprehensive, nor to provide legal advice. Should you have any questions on issues reported here, please get in touch. © 2026 Linklaters.

Linklaters LLP is a limited liability partnership registered in England and Wales with registered number OC326345. It is a law firm authorised and regulated by the Solicitors Regulation Authority. The term partner in relation to Linklaters LLP is used to refer to a member of the LLP or an employee or consultant of Linklaters LLP or any of its affiliated firms or entities with equivalent standing and qualifications. A list of the names of the members of Linklaters LLP and of the non-members who are designated as partners and their professional qualifications is open to inspection at its registered office, 20 Ropemaker Street, London, EC2Y 9AR, England or on www.linklaters.com and such persons are either solicitors or registered foreign lawyers. Please refer to www.linklaters.com/regulatory for important information on our regulatory position. LIN.GBR.781.26