

Outlook for digital
markets regulation
in 2024

Outlook for digital markets regulation in 2024

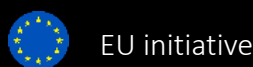
At the start of 2024, during an unprecedented time of regulatory activity relevant to the digital economy, against a backdrop of continuing geopolitical change, we have set out our view of digital markets regulatory themes relevant to competition and consumer protection issues which we expect to be particularly important for the year ahead. This outlook, approached from UK and EU perspectives, is primarily written for Boards and Senior Executives of large digital and technology companies. It is also relevant to companies in different industry sectors who have a retail presence in online markets and those who rely on 3rd party digital service provision (e.g., cloud) as part of their operations.

The key regulatory topics we have identified, in no particular order, are:

- 1. Online safety: bedding in the new user protection regimes
 - 2. Digital markets competition: initial changes felt
 - 3. Opening up the data economy: the time is now
 - 4. Cloud competition: European implementation begins
 - 5. Digital sovereignty: expansion driven by geopolitical concerns
 - 6. Third party digital assurance: first audits to test the regimes
 - 7. AI: regulatory implementation and test-case enforcement
 - 8. Making the digital (net) work: potential regulatory interdependencies
 - 9. Digital advertising: new requirements bite, further intervention possible
 - 10. Financial services: blurred boundaries, risks and opportunities
- Spotlight on: online choice and dark patterns

For each topic, we highlight:

The relevant regulation or potential regulatory initiative:



The area(s) of the digital markets ecosystem that will be particularly affected (please see Appendix I for a full description of the types of companies in each area):



Connecting



Content



Trading



Enabling



1. Online safety: bedding in the new user protection regimes

Landmark new online safety rules will apply in full in the EU, with Ofcom's implementation of equivalent regulation likely to progress quickly in the UK. Company compliance will pick-up pace accordingly. External events will continue to play an important role in shaping enforcement of the new rules, with regulators testing their new powers to address online disinformation, especially relevant with elections taking place in a significant number of countries during 2024. These new requirements necessitate a step-change in compliance. Internet companies within scope will need to continue to evolve and adapt their operations, control functions and governance structures accordingly, in particular given the new sanctions that authorities have at their disposal.

Full application of new EU rules and speedy implementation of the UK equivalent requires a significant response by the many online companies within scope.

In the EU, the new risk assessment process for the largest internet companies under the [Digital Services Act](#) ('DSA') will become more mature, with ongoing publication of bi-annual transparency reports by the largest platforms and completion of the first audits. Publication of the first comprehensive annual review by the new European Board for Digital Services will also occur.

We expect to see increasing activity by those third-party bodies tasked with specific roles under the DSA, such as the newly created [European Centre for Algorithmic Transparency](#), which has a key role to provide scientific and technical expertise relevant to algorithmic transparency and accountability. Access to very large online platform and search engine data relevant to system risks by "vetted researchers" will also be a strategically significant – and potentially contentious - topic for both platforms and the third parties that will request this data. A European Commission Delegated Act on this topic is foreseen by April 2024, which should provide stakeholders with more information on how this process will work in practice.

We also expect to see an increased emphasis on how use of RegTech can address online safety regulatory compliance, in particular children's online safety. This has specific relevance in the context of child safety topics such as age verification and safety by design.

The largest internet companies already within scope will need to remain agile as the European Commission flexes its new oversight responsibilities (as already seen in December 2023 with the investigation into a Very Large Online Platform's ('VLOP') compliance with certain provisions of the DSA including those related to risk management, content moderation & dark patterns). As of 17 February 2024, DSA rules will also apply to a much broader range of online companies (those with over 50 employees and whose turnover exceeds EUR 10 million in the EU), with new 'Digital Services Coordinator' leads also being designated at Member State regulatory authorities to enforce compliance. This is also likely to result in a transitional period for the companies within scope, given the regulatory bodies (in some cases newly established) will also be considering how best to exercise their new responsibilities.

Relevant regulations:



Digital Services Act



Online Safety Act

Impacted areas:



Connecting



Content

Companies will need to develop their operations and control functions to comply with a wide range of new obligations, ranging from cooperation with trusted flaggers to complaints handling and vetting of third-party suppliers.

Following on from this, the cumulative impact of related, but distinct, online safety regulation should be assessed. In Ireland for example, in addition to its Digital Services Coordinator role under the DSA, the newly established Coimisiún na Meán, issued a [consultation](#) in December on the Online Safety Code to support the existing Online Safety and Media Regulation Act 2022. In the UK, the Age Appropriate Design Code has potential crossovers with the Online Safety Act ('OSA') as well as with [work](#) in the EU to codify similar principles. Global firms will need to navigate their way through such requirements.

In the UK, we expect Ofcom to continue at pace to [implement](#) its new responsibilities under the recently finalised OSA, with further detail being provided on important topics such as illegal content and children's risk assessments. This also signals a step-change in the level of governance that will be required, for example due to the changes in online company governance and new senior manager responsibility requirements associated with the new regime (something we have already written about [here](#)). New operational requirements will come through thick and fast. Taking just one example, Ofcom intends to finalise its guidance on illegal risk assessments in Autumn 2024. From this point, internet companies within scope will need to carry out their first assessment within three months.



2. Digital markets competition: initial changes felt

As with online safety, landmark new competition rules are now established for digital markets in the EU, with political scrutiny of equivalent regulation – the Digital Markets Competition and Consumers Bill – progressing in the UK. We expect that the EU gatekeeper designation process – which currently regulates core platform services of six large digital platforms in the EU, and which has been running through most of 2023 – will start to deliver some initial changes to competition in digital markets. The compliance reports to be published during 2024 should also trigger further rounds of feedback with the business users and other market participants who stand to benefit from the DMA’s goal to ensure fair and contestable markets in the digital sector. In the UK, it is expected that the equivalent digital competition rules will receive Royal Assent in Spring 2024, paving the way for the CMA’s Digital Markets Unit to get going in earnest.

The initial market impact of changes to Gatekeepers’ business models will start to be felt in the EU, more changes will be required if the European Commission thinks they don’t go far enough.

It is worth recalling that the philosophy behind the EU [Digital Markets Act](#) (**‘DMA’**) is to move to an ‘ex-ante’ digital markets regulatory regime, away from the more adversarial ‘ex-post’ process which is often characterised by lengthy investigations and limited transparency. The coming year may provide the first real opportunity to assess whether or not this vision is on its way to becoming a reality. The submission of the first gatekeeper compliance reports by 7 March 2024, and subsequent publication of non-confidential summaries by the European Commission, will shed light on the behavioural changes that have (or have not) started to happen relevant to the regulatory obligations. The outcomes of the appeals to the European Court of Justice filed by certain companies against their gatekeeper designations are also keenly awaited.

In terms of operational implications, gatekeepers will continue to be under the microscope regarding their compliance with the new obligations, albeit with an opportunity to demonstrate that their practices fall on the right side of the rules (e.g., through effective testing for online choice architecture in the context of the self-preferencing prohibition).

On a number of topics (e.g. communication with consumers about their ability to switch to competing platforms, provision of information to business users on costs and metrics of digital advertising) we expect to start to see some early changes in market dynamics (recognising that the provisions of the DMA will require ongoing implementation, engagement and review).

On others, it remains to be seen. For example, will the envisaged process allowing app developers to utilise third party payment systems as an alternative to gatekeeper payment systems work in the way that third parties expect? Will the new data transparency requirements, particularly the requirements to enable "authorised third parties" to access users' data, enable innovation and new digital services? If the compliance report process results in the Commission taking the view that there has been insufficient progress by the gatekeepers in question, further investigations or market studies seem likely.

Relevant regulations:



Digital Markets Act



Digital Markets Competition and Consumers Bill

Impacted areas:



Connecting



Content



Enabling



Trading

In the UK, it is expected that the [Digital Markets Competition and Consumers Bill](#) ('DMCCB') will finally become law in 2024 (with a recent Competition and Markets Authority ('CMA') [overview](#) assuming a Royal Assent date of April 2024, followed by final CMA guidance in October 2024 and the first designations of companies with 'Strategic Market Status' in July 2025). Interested parties will be closely watching the EU process in order to leverage any learnings with the CMA.

There is a read-across between the services relevant (or potentially relevant) to digital markets competition and the policy objectives underpinning the digital policy topics set out in other sections of this document. Immediate areas of overlap exist with respect to data, advertising and cloud. Looking forward, we also expect to see further debate regarding the extent to which AI functionality (in particular Large Language Models) may become a cause for competition concern in digital markets. It is notable that the first trend highlighted in the [CMA's Trends in Digital Markets report](#), published in December 2023, related to the rapid and widespread deployment of AI foundation models and the potential harms to competition and consumers that could result. The European Commission has also kicked off a [competition review of generative AI](#) in early January. The relevant authorities will be keeping a close eye on how the market develops in this regard.



3. Opening up the data economy: the time is now

The EU Data Act, finalised in late 2023 hot on the heels of the previous year's EU Data Governance Act, intends to address the challenges and opportunities presented by data in the EU, underpinned by a new ex-ante regulatory regime. Indeed, the European Commission has calculated that in 2028, the economic impact of the Data Act could imply an increase in GDP of 273 billion EUR (representing an additional 1.98% of GDP). The Data Act raises a wide range of different strategic and operational risks and opportunities for companies across the economy. The focus is now on implementation, which raises profound operational questions for the many different companies within scope. The sector-specific UK 'Smart Data' equivalent should be introduced as part of the Data Protection and Digital Information (No 2) Bill, which is expected to become law in 2024.

The ambitious EU regulatory framework is in place and the focus will shift to the significant company implementation required to unlock the economic benefits it has been designed to realise.

There are few that would argue that the EU [Data Act](#) is not an ambitious, yet complex, regulation. It has many different elements, with the business-to-consumer ('B2C'), business-to-business ('B2B') and business-to-government ('B2G') data sharing provisions of particular relevance to the market. The European Commission, as well as the competent authorities and/or data coordinators that will be designated at Member State level, will have important roles to play in bringing the provisions to life. Taking the example of B2B data sharing, the EU Data Act now sets out a framework that such data should be shared on fair, reasonable, non-discriminatory and transparent terms. There is a clear case for an appropriate body to provide guidance on how these terms should be applied, and of course this is already a task assigned to the European Commission under the Data Act. We would expect guidance on this to be provided during the year.

The potential implications across the Data Act as a whole are vast and new operational and governance processes relevant to the various data sharing scenarios enshrined in the Data Act will need to be established. Companies should be reviewing their own operations in light of these new rules, conducting analyses of the strengths, weaknesses, strategic opportunities and threats associated with the new rules. Taking just three examples; from a B2B perspective, how should an automotive manufacturer respond to a request by an aftermarket supplier for access to in-car data? From a B2C perspective, how should a manufacturer of connected video doorbells respond to a data request from a consumer for access to the functioning of their device? From a B2G perspective, how should a supermarket respond to a request from a public sector body for data in the event of a public health emergency?

The strategic and operational implications of the EU Data Act relevant to the different data sharing scenarios should be considered now. The regulation should also be assessed in conjunction with the AI Act, given that trusted mechanisms for the re-use, sharing and pooling of data are essential for the development of data-driven AI models.

Relevant regulations:



Data Act



Data Governance Act



Data Protection and Digital Information (No 2) Bill

Impacted digital markets:



Connecting



Enabling



Trading

In the UK, focus will be on the Part 3 ‘Smart Data’ provisions of the [Data Protection and Digital Information \(No 2\) Bill](#), designed to facilitate private sector data sharing. These provisions, expected to become law in 2024, are more targeted than the “horizontal” provisions of the EU Data Act and envisage implementation across specific sectors of the economy. Indeed, the “Smart Data Big Bang” announced in the [Chancellor’s Autumn Statement](#) confirmed a focus on using these new powers in the following seven sectors: energy, banking, finance, retail, transport, homebuying and telecoms. We expect this to remain a key area of government and policymaker priority, and companies in these sectors in particular should monitor developments and prepare accordingly.



4. Cloud competition: European implementation begins

New EU rules have recently been agreed at EU level designed to address customer ‘lock in’ and open up the cloud services market to competition. These rules will require significant implementation ahead of their application at the end of 2025, which we expect to kick off in earnest during the year ahead. At UK level, we expect to see a crystallisation of the CMA cloud services market investigation following Ofcom’s referral, with a provisional decision expected in Autumn 2024.

Service provider implementation of the new EU cloud switching rules will need to begin in earnest, with the ultimate direction of travel in the UK also becoming clear.

If the new EU framework (introduced as part of the [Data Act](#)) works as envisaged, it should deliver real change; opening up the market to increased competition, eliminating switching charges and reducing porting timescales. However, as we have previously [written](#), there will need to be a journey to get the desired regulatory outcome, as demonstrated by the timescales in question (e.g., removal of egress charges within three years following the regulation entering into force, which means early 2027).

Strategic planning relevant to implementation should, therefore, start now. The practical challenges of implementation cannot be underestimated, with just one example being the new regulated switching timescales now in place (switching within 30 days, albeit with an extension being allowed if this is not “technically feasible”).

This will require cloud service providers to establish new operational and governance processes to oversee compliance. Customers of cloud services should already be considering their future cloud procurement strategies with these new obligations in mind. Providers should also be developing their commercial strategies given, for example, the requirements to adjust pricing consistent with the new rules.

Continued activity to set up the oversight regime in the EU is to be expected, including by the European Commission, the European Data Innovation Board and the competent bodies that will be designated at national level. Dialogue with the relevant authorities will be key; further regulatory guidance would no doubt be welcomed, but it remains to be seen how much will, in practice, be offered.

Relevant regulations:



Data Act



CMA Cloud Services
Market Investigation

Impacted area:



Enabling

In the UK, the CMA [market investigation](#) will continue consistent with the procedural requirements associated with a process that has such significant market remedies at its disposal. It is not expected to conclude by the end of the year, but a provisional decision is expected, which will indicate the direction of travel. Given the year-long Ofcom market study that preceded the CMA's current investigation, it seems very likely that whatever the outcome, any requirement for ongoing regulatory oversight— including via any additional powers conferred by the Digital Markets Competition and Consumers Act, if it becomes law in time - will have been baked into the final decision.



5. Digital sovereignty: expansion driven by geopolitical concerns

The concept of ‘sovereignty’ (broadly speaking, the ability of a country or region to assert autonomy over key elements of its digital infrastructure and/or operations) has underpinned numerous national and regional digital policy initiatives in recent years. Significant regulatory policy discussions have taken place in areas such as 5G network vendor diversity and cloud computing. We expect these discussions to deepen, and become more diverse, during the year ahead, driven by ongoing geopolitical uncertainty and the pivotal relevance of digital technology across society and the broader economy. The need for companies to “think globally, act locally” is more important than ever.

The prevalence of digital technology, combined with continuing geopolitical concerns, means that companies should prepare for a broader range of operational restrictions imposed with sovereignty in mind.

In the UK, the creation of the Department for Science, Innovation and Technology (‘DSIT’) in February 2023, and its subsequent [focus on the five key technologies](#) that are most critical to the UK (namely AI, future telecommunications, semiconductors, quantum computing and engineering biology) is a vivid illustration of just how central digital technology is seen as being to a country’s success and future prosperity. Similar objectives have underpinned the current EU mandate, with the [European Commission’s critical technology areas for EU security in October 2023](#) honing in on a list focused on advanced semiconductors, artificial intelligence, quantum and biotechnologies.

These priorities will continue to inform a number of new initiatives during the year – including risk assessments at EU level to be carried out primarily by the European Commission and Member States, with input from the private sector. The Commission has stated it will be a dynamic and continuous process which will include consideration of risks in these areas relevant to the resilience of supply chains, physical and cyber security of critical infrastructure, technology security and technology leakage and weaponisation of economic dependencies or economic coercion. Companies active in the abovementioned areas should therefore prepare themselves for potential information gathering by the bodies concerned. Such activity will help set regulatory policy priorities going forward and companies across the economy using this technology in their operations should be mindful of this activity given potential impact on their operational strategies going forward.

The example of Cloud Computing remains a live example of how an emphasis on the need for ‘sovereign technology’ can feed into the regulatory debate. In this case, concerns about sovereignty manifested themselves in the nationality of companies that can – or cannot - provide different cloud services in the EU consistent with the European cloud certification scheme under the [EU Cybersecurity Act](#). This challenging discussion has highlighted the difficulty of factoring in (ostensibly geopolitical) considerations into day-to-day regulatory policy. One which major global cloud providers, through partnerships with local digital companies and marketing of ‘sovereign’ cloud solutions, have already sought to navigate.

Relevant regulations:



EU Cybersecurity Act, with other initiatives on horizon



Data Act



Data Governance Act

Impacted areas:



Trading



Enabling

The example of [EU Data Spaces](#), a key part of the EU's strategy to ensure Europe's data sovereignty, is another relevant example in this respect. Fourteen Data Spaces have been identified to date, including those focused on mobility, health, financial and manufacturing data.

So, what does this mean for the global companies whose digital service provision may be particularly affected by this debate? We see three key actions. First, stay close to the political and policy discussions to understand such concerns, with effective External Affairs/Public Policy functions being more important than ever. Second, demonstrate the broader social and economic benefits of company activity in the geographic area that might be affected by "sovereignty regulation" to policymakers who may be developing regulation with sovereignty considerations in mind. Finally, build in sufficient operational flexibility into operating models and/or pursue partnership strategies to address potential sovereignty requirements (e.g., locally hosted digital operations and/or infrastructure).



6. Third party digital assurance: first audits to test the regimes

In the next year, we will see the first outcomes of the new audit requirements that have already been introduced into digital markets at EU level. This will be an important opportunity for companies to test and refine their approach in dialogue with both third party experts as well as the Commission and other relevant authorities. At UK level, algorithmic auditing will be a priority for the DRCF's work and we expect to see further guidance from the UK authorities, on topics such as common standards for third party review and benchmarking. These are examples of areas that companies should focus on now, given impacts on future company governance and control functions.

Regulators will continue to pioneer the use of external audit and assurance in order to drive compliant company behaviour.

Third party assurance has, of course, been a central element of the financial services regulatory system for many years. To date, it has not been widely practiced in broader competition and consumer protection regulation. However, it is now being pioneered in digital markets regulation too, for example under the DMA, DSA and AI Act.

Under the DMA, gatekeepers are required to submit an audit in respect of consumer profiling by March 2024. It is notable that there are different views in the market as to how prescriptive the guidelines for conducting such audits should be, with the Commission (arguably) currently preferring a more flexible approach. The first audits should shed light on whether this policy provides the certainty that is required. Impacted companies should be prepared to articulate their views in this respect. Under the DSA, independent auditors are required to assess (at least once a year) compliance of VLOPs and Very Large Online Search Engines ('VLOSEs') with all DSA obligations. The first DSA audit report is due in August 2024.




The European Commission is expected to bring a number of Codes of Conduct into scope for the year two audit including for example the [Code of Practice on Disinformation \('COPD'\)](#) which will add to the existing obligations under the DSA.

There is also a broader trend that can be seen in this area, perhaps receiving less attention than the examples above. Recent competition investigations (for example relevant to digital advertising markets and online marketplaces) closed by the CMA on the basis of commitments have included a role for a third party "monitoring trustee" to provide assurances that the companies under investigation have complied with their obligations. This has included overseeing the implementation of new technical systems and employee training. Given the information asymmetries at play between regulators and the digital companies they regulate, the differences in resources and the fast-moving nature of digital markets, this trend may be expected to continue. Companies should prepare themselves for such an eventuality.

Relevant regulations:

-  Digital Markets Act
-  Digital Services Act
-  AI Act
-  Online Safety Act

Impacted digital markets:

-  Connecting
-  Trading
-  Content

One area where this may manifest itself is during the implementation of the OSA. The OSA also envisages a role for Ofcom to obtain skilled persons' reports with respect to company compliance, which could also be relevant in this context. Indeed, the FCA is already able to commission a "skilled persons" report. It is notable that the Digital Regulation Collaboration Forum ('DRCF') has confirmed in its [guidance](#) that this provision might be used in the context of algorithmic auditing.

Overall, these regulatory trends will require changes to governance and control functions going forward. Indeed, given this direction of travel, companies should already consider whether they may wish to adopt a pro-active approach to obtaining such assurance, potentially in lieu of a formal requirement being imposed at a later stage by a regulatory body.



7. AI: regulatory implementation and test-case enforcement

The political and regulatory debate will continue. However we expect a shift in focus in the debate from ‘how to regulate’ (itself prompted by the emergence of GenAI during 2023) to a regulatory discussion focused on company preparedness and prioritised test-case enforcement.

A shifting of emphasis from rule design to company preparedness in the EU and adherence to existing regulatory requirements in the UK.

At international level, cooperation on AI came to a head during 2023, with milestones such as the agreement of the [G7’s International Guiding Principles on Artificial Intelligence](#), formation of [UN’s High Level Advisory body on AI](#) and the [UK’s initiation of the new AI Safety Summits](#) (which will continue through 2024).

The devil is, of course, in the detail and at a national and regional regulatory level, we can observe a variety of different approaches. In the EU, late 2023 saw the political agreement of a new [AI legislative framework](#). As we have [written](#), the AI Act is set to become law in the first half of 2024, with a two-year phased implementation period then commencing before it becomes fully enforceable in 2026. In the UK, in the context of the government’s decision not to introduce specific rules to regulate AI, sector regulators honed in on their AI responsibilities, particularly via the DRCF.

From a regulatory perspective, during 2024 we broadly expect EU authorities to focus on implementation of the new AI regulation and UK authorities to test the application of existing regulatory regimes to AI. For multi-national firms this will require navigation, with regulatory strategies and associated operational and governance processes being set accordingly.

Under the EU regulation, companies should assess which of their current and planned AI systems and models fall in scope of the AI Act and conduct a gap analysis against key requirements. This will provide insight into the scale and challenge of compliance efforts and help identify the impact of the AI Act on strategic choices and product governance. Organisations should develop their overall AI strategy, refining it as more details emerge during 2024 (closely monitoring, for example, the emergence of the required technical standards) and through the implementation phase.

Relevant regulations:



AI Act



AI framework leveraging and testing existing rules

Impacted areas:



Connecting



Content



Enabling



Trading

The AI Act also encourages individual Member States to establish regulatory sandboxes, according to a common set of rules to promote standardised approaches across the EU. Indeed, Spain has already launched the EU's [first AI Regulatory Sandbox pilot](#) which aims to operationalise AI Act requirements.

In the UK, we expect regulatory authorities to prioritise activities which seek to demonstrate the application of existing regulatory frameworks to AI. Companies should prepare for further regulatory activity, ranging from new policy programmes and information gathering, to potential enforcement. We've already identified the CMA's focus on foundation models in the competition section of this outlook. From a consumer protection perspective, activity could include testing of the Consumer Rights Act (which may protect consumers where they have entered into a sales contract for AI-based products and services) or existing product safety laws (with the aim of ensuring that goods that include integrated AI are safe). From a sectoral perspective, this could include consideration of how to address deep fakes in the context of Ofcom's illegal harms duties under the OSA, use of the 'skilled person' powers by the Financial Conduct Authority ('FCA') in the context of algorithmic auditing and the FCA addressing AI risks via the Consumer Duty framework. Any gaps will clearly be closely observed by the authorities in question, with the potential for future rulemaking not being excluded.

Companies active in the UK should also follow the progress of the new [AI and Digital Hub](#) and consider their engagement strategies accordingly. This service, to be piloted by the DRCF, is intended to bring together the different regulators involved in the oversight of cross-cutting AI and digital technologies, with the aim of helping companies develop ideas with regulatory compliance in mind. The service will launch in the first half of 2024 for a 12-month pilot.



8. Making the digital (net) work: potential regulatory interdependencies

A notable element of recent communications policy in both the UK and the EU has been the regulatory interplay between companies in the content, online services and connectivity segments of the value chain. This has manifested itself most publicly in the ‘fair contribution’ debate. Proposals in the UK Digital Markets Competition and Consumers Bill also envisage the creation of a new regulation to require payments from digital platforms to news publishers for their content. Commissioner Thierry Breton’s October 2023 announcement of a forthcoming Digital Networks Act would appear to signal further regulatory activity at EU level, albeit with the detail yet to be determined. What this means for the different players in the value chain is expected to be much debated over the coming year. Companies should develop their strategies accordingly.

Interdependencies between the content, online services and connectivity segments will continue to stimulate regulatory debate, necessitating ongoing strategy review by the companies concerned.

With 2024 being the final year of the current European Commission mandate, discussions are afoot in Brussels as to what topics should be prioritised from 2025 onwards. Commissioner Breton has already [signalled](#) that there needs to be an emphasis on ensuring fit for purpose networks and a new Digital Networks Act “to redefine the DNA of our telecoms regulation”, so that the EU can achieve success in areas such as AI, data and the metaverse. This begs the question of what will be included within the scope of such an ambitious proposal. Companies in the content, online services and connectivity segments should be sharing their wish-lists on what should, or should not, be prioritised.

Net Neutrality is of course a key regulatory file in relation to the relationship between connectivity providers and online companies. The [outcome of the recent UK review](#) of Net Neutrality regulation didn’t signal any major reform of the previous EU-influenced regime (also essentially unchanged in the EU following the Commission’s 2023 review, although now under [review again by the FCC](#) in the US). The Ofcom review also didn’t signal any immediate movement on the ‘fair contribution’ debate (i.e., whether connectivity providers should be allowed to directly charge content and online service companies for carrying internet traffic) at UK level.

Interested players should also monitor the political debate on the DMCCB’s provisions which could enable the Digital Markets Unit to regulate the terms on which news publishers may charge large internet platforms for carrying their content. This is a trend which is already prevalent in other international markets such as Canada and Australia. There are many similar arguments being made in the context of this discussion and the ‘fair contribution’ discussion.

Relevant regulations:



Potential Digital Networks Act



Digital Markets Competition and Consumers Bill



Net Neutrality

Impacted areas:



Content



Enabling



Connecting

Indeed, it is also being extended into AI, for example, whether online services companies should be required to pay content providers for content included in large language models.

To sum up, there are multiple commercial interdependencies across the internet ecosystem. Following the initial raft of digital markets regulation, we expect to see continued cases being made for intervention to regulate large internet companies in other areas of the internet ecosystem. Although regulators will no doubt need convincing, regulatory change would be expected to fundamentally alter these existing relationships. Regulatory strategies should continue to be developed throughout the course of the year ahead.



9. Digital advertising: new requirements bite, further intervention possible

Advertising fuels online markets, with increased growth predicted in the year ahead. But there remain concerns about competition, trust and accountability in the sector. Much policy work has already been done to address this in both the EU and the UK (as demonstrated by the existing provisions relevant to online advertising in both the EU DSA and DMA and also the OSA in the UK). However, further specific regulatory intervention is on the cards, given advertising specific studies already undertaken at EU and UK level. On top of that, 2024 looks to be the year where the “post cookies world” finally becomes more of a reality, with the privacy and competition considerations that will result. Advertisers, publishers and online companies alike should prepare for further regulatory change.

2024 is lining up to be a significant year for regulatory developments in the sector, given application of new competition and consumer rules and potential for further targeted intervention.

[According to WARC](#), global ad spend will significantly increase in 2024, growing at 8.2% as opposed to 4.4% in 2023. This is an area that can raise a multiplicity of different regulatory concerns, including privacy, consumer protection (e.g., fraudulent advertising), online safety (e.g., inappropriate advertising to children) and competition (e.g., given the strong position of a small number of large platform companies in the ecosystem).

Given the recommendation included in a [European Commission initiated study published in 2023](#) that there is “a strong case to reform digital advertising...the status quo is unsustainable for individuals, publishers and advertisers”, it would not be entirely surprising if further steps to promote competition in the advertising market featured in the next Commission mandate, especially if the provisions in the DMA are not deemed to have had significant enough effect. The first DMA compliance reports are keenly awaited in the context of the discussion on how advertising services product definitions are treated (a part of the product? a separate product?) given the impact the requirements could have in separating them from their crucial resource: data. The reports should shed light on how gatekeepers are complying with the ad-focused requirements.

In the UK, pro-competitive advertising measures are also likely to be a priority under the Digital Markets, Competition and Consumers Act following anticipated Royal Assent of the Bill later this year. The outcomes of the ongoing EU and US antitrust investigations relevant to digital advertising are also keenly awaited.

From a competition perspective, we see three trends for companies to watch. First, we expect the regulatory manoeuvring around a post-Cookies world to continue, in light of the regulatory intersection between competition and data protection and the ongoing review of the Privacy Sandbox in particular. Second, policymakers will be closely analysing market shares in the digital advertising market, to assess whether there are serious challenges being mounted to the established players (e.g., via the recent AdTech joint venture in the European telco sector).

Relevant regulations:



Digital Market Act



Digital Services Act



Online Safety Act



Digital Markets Competition & Consumers Bill



Other initiatives on horizon

Impacted areas:



Connecting



Content



Enabling



Trading

Third, the dynamics between large digital platforms remains one to watch; it is notable that one of the points made by a company appealing its gatekeeper designation in November 2023 is that this designation actually *diminishes* the prospect of it mounting an effective challenge to other designated gatekeepers in the online advertising space.

From a consumer protection perspective, immediate focus will be on the DSA's ad transparency obligation, ahead of applicability to VLOPs and VLOSEs on 17 February 2024. This requirement ensures that users have information about the ads they are presented (e.g., that the ad is indeed an ad, and the main parameters that have been used to determine the recipient of the ad). Compliance will in many cases require interaction with other elements of the supply chain in order to populate the disclosures. Product roadmaps will require continuous review and updating based on initial implementation learnings. Overall, companies in the ecosystem should ensure that systems, processes and governance are kept under review, in particular as the DSA transparency provisions start to bite.

The UK government has also recently confirmed it intends to introduce a [new and targeted regulatory framework for online advertising](#), which focuses on tackling illegal advertising (as defined under existing criminal provisions) and increasing the protection of under-18s online. Platforms should also prepare for further scrutiny in these areas.



10. Financial services: blurred boundaries, risks and opportunities

There is a significant amount of new financial services regulation that will be implemented or debated over the coming year. Technology companies will need to navigate regulation in areas such as stablecoins, critical third-party providers and financial data access. The boundaries between 'digital' and 'financial services' regulation continue to blur, generating both risks and opportunities for large internet and technology companies in the process. A multi-faceted approach, covering strategy, governance and operations, will be required so that technology companies can deliver to increasing regulatory expectations as they expand their business into financial services.

There is a significant body of new and emerging financial services regulation relevant to large internet and technology companies not 'born' in the sector, creating both opportunities and risks, meaning that a mapping of the risks and opportunities is required.





The continued evolution of the financial services regime in light of technological development is, of course, nothing new. What has been apparent in recent years, however, is not just an increasing convergence between the two regimes, but also large internet and technology companies being directly or indirectly regulated under the financial services regime.

We see three areas as being particularly relevant. First, where large internet companies are currently undertaking activities that are not regulated (e.g., in relation to some digital assets), but which will become regulated. Second, where supervisors are concerned large internet companies' direct / indirect role in controlling access or choice to financial services (e.g., payments) or data is creating distortions in the market (e.g., in the context of data markets). Third, where large internet companies are not performing financial activities per se, but where their tech services are seen as so critical as to call for direct supervision (as evidenced in the Operational Resilience regime). We elaborate on each of these areas below.



In relation to digital assets, new EU and UK regulatory frameworks for stablecoins may enable non-financial services firms to explore providing regulated stablecoin services, e.g. wallets and integrated payment services (something which we have previously written about [here](#)). Large internet companies should be aware of new and emerging EU and UK rules, and the need to seek authorisations with the financial services regulators. In some cases, depending on the scale of growth plans, these companies may be subject to oversight by multiple regulators. e.g., in the UK, not just the FCA, but also the Bank of England.

Under open banking, large internet companies are already able to take advantage of existing provisions for market entry as either an Account Information Service Provider ('AISP') or Payment Initiation Service Provider ('PISP'). Regulatory bodies are keen to expand this regime further, and in time, expand data-sharing requirements to other products and services via open finance. One such example is the opportunity for new market entry which could also arise under the EU's proposed [Financial Data Access \('FIDA'\) framework](#), essentially the legislative backbone for the EU implementation of open finance (something which we have previously written about [here](#)).

Relevant regulations:

-  Digital Operational Resilience Act (DORA)
-  Financial Data Access Framework
-  Markets in crypto-assets regulation (MICA)
-  Critical third-party regime

Impacted digital markets:

-  Trading
-  Enabling

In saying that, this activity will be closely observed by the applicable regulatory bodies. If large internet companies are perceived to be acting as “data gatekeepers”, this may prompt regulators to introduce safeguards in the next steps of open banking and open finance. For example, FIDA’s initial proposal is that if a data user is part of a larger group, only the specific entity authorised as a data user will be able to access and use the customer data. In the UK, the FCA recently launched a [call for input](#) in this area.

In relation to operational resilience, in the EU, implementation of the [Digital Operational Resilience Act](#) (‘DORA’) will continue. In the UK, the FCA is expected to consult on a centralised register for collecting information on financial firms’ outsourcing and third-party arrangements. Once operational, this will help to inform the designation process to identify the [critical third parties](#) (‘CTPs’) to the UK financial services sector. For those large technology companies that provide services to financial services firms, whether cloud service provision, AI or quantum computing, this should be on their radar. In summary, a strategic mapping of these different initiatives, combined with an assessment of the potential strengths, weakness, opportunities and threats associated with each, will enable technology companies to define their position, enter new markets, and manage the implications accordingly.



Spotlight on: online choice and dark patterns

There are numerous recent examples, at both UK and EU level, of regulators prioritising concerns relevant to use of online choice architecture (broadly speaking, how the design of online environments affects consumer decision making and actions). We expect to see a range of very practical examples of how regulators are prioritising this area over the year ahead, ranging from continued industry dialogue and policymaking to targeted enforcement action.

Regulatory concerns relevant to online choice architecture underpin different provisions of the DSA (relevant to use of so called ‘dark patterns’), the DMA, the existing consumer protection regime in both EU and UK, the proposed Digital Markets Competition and Consumers Act in the UK and also recent activity by the Federal Trade Commission in the US. A number of different examples of online choice architecture are set out in [Figure 1](#) below. Inherent within much of the regulatory guidance is that companies should ensure they have the processes in place to be able to test for ‘good’ online choice architecture relevant to a customer’s digital journey. This means that companies should be able to demonstrate that users are being treated fairly when making online purchasing decisions (e.g., that there is sufficient transparency around pricing or that purchasing options are displayed in a “fair” way).

It is also relevant to online scenarios such as the process to subscribe and unsubscribe (with the same level of ease), from products and services. Companies, both digital platforms as well as “traditional” firms with an online presence, such as supermarkets, airlines, digital content businesses, for whom online transactions are an important part of their revenue, should review, and where required update, their operations and processes to ensure they are consistent with positive customer outcomes.

Figure 1: OCA practices - illustrative examples

	STRUCTURE					
		DEFAULTS	Pre-defined settings		SLUDGE	Excessive friction
		RANKING	The order of options		VISUAL MANIPULATION	Visual features used to steer choices
		BUNDLING	Several items merged into one			
INFORMATION		PRICING	Steering users through prices (e.g., reference pricing, drip pricing, etc.)		INFORMATION OVERLOAD	An excessive amount of information purposely confusing users
		FRAMING	The way information is presented to users			
PRESSURE		SCARCITY & POPULARITY CLAIMS	Pressuring users via claims (e.g., limited stock, high popularity)		TIMING & FREQUENCY OF PROMPTS	Inducing actions at specific moment(s) and at specific intervals
		PERSONALISATION	Individually tailored offers to steer choices			

This includes putting in place appropriate testing and control functions where required.

We set out below three different scenarios which highlight regulatory concerns about ensuring fair online choice architecture, as follows:

- Ensuring internet fair product search under the self-preferencing prohibition of the DMA (Figure 2).
- Ensuring fair online purchasing under the DSA via online platforms making information available to consumers about online traders (Figure 3)
- Online supermarkets ensuring compliance with general consumer protection regulation by ensuring that consumers are not misled (Figure 4)

Figure 2: internet product search

DMA – Article 6(5): companies in scope must not treat their services and products more favourably than similar services or products offered by a third party. Companies must apply transparent, fair and non-discriminatory conditions to ranking.

User shopping third-party (TP) products/services from a large company's online marketplace.

RELEVANT OCA AREAS

Ranking: the way options are ranked influences user choice, with the first few options in any online search list being the most likely to be selected. Companies in scope need to strike the right balance between own self-interest (e.g., selling own products and providing visibility to some TP products) and overall relevance.

Framing: information should not be framed in a way that manipulates user choices away from their best interest. In this case, users should be able to find the products/services they want to buy and not just what the company wants to sell them.

Personalisation: personalisation of search results according to data gathered on the users' interests should not be employed in a way that unfairly tricks users towards/away from specific choices.

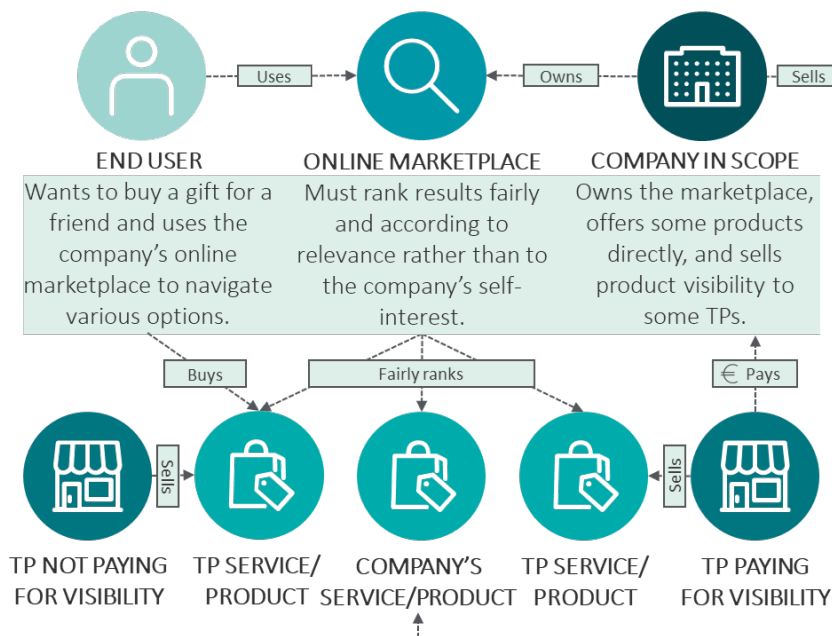
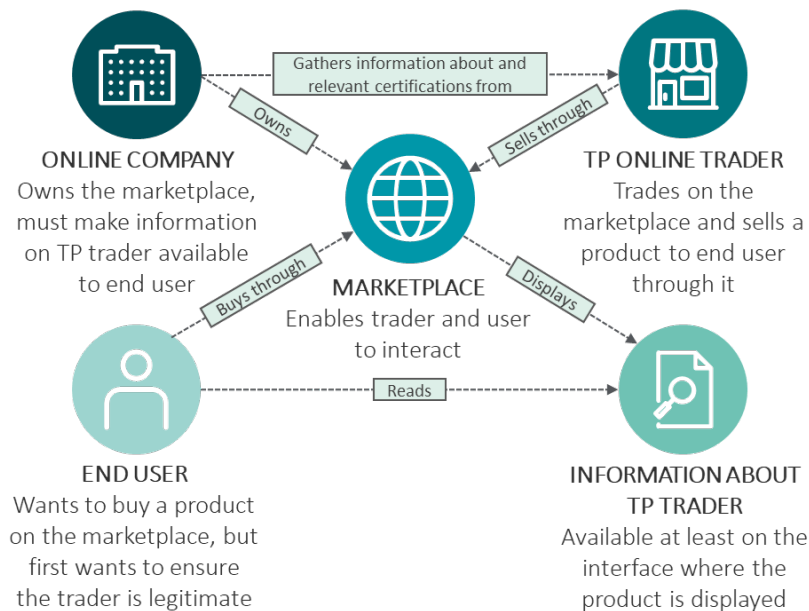


Figure 3: online purchase

DSA – article 30(7): provider of online platforms allowing consumers to conclude distance contracts with traders shall make information about the trader available on its online platform to the recipients of the service in a clear, easily accessible and comprehensible manner.

User accessing information on a third-party (TP) trader through an interface provided by the online marketplace.



RELEVANT OCA AREAS

Information overload: the interface should not provide too much detail in a way that tries to hide or makes it difficult for users to find the relevant information required by law on third party traders. At the same time, information should not be excessively oversimplified by providing too little detail.

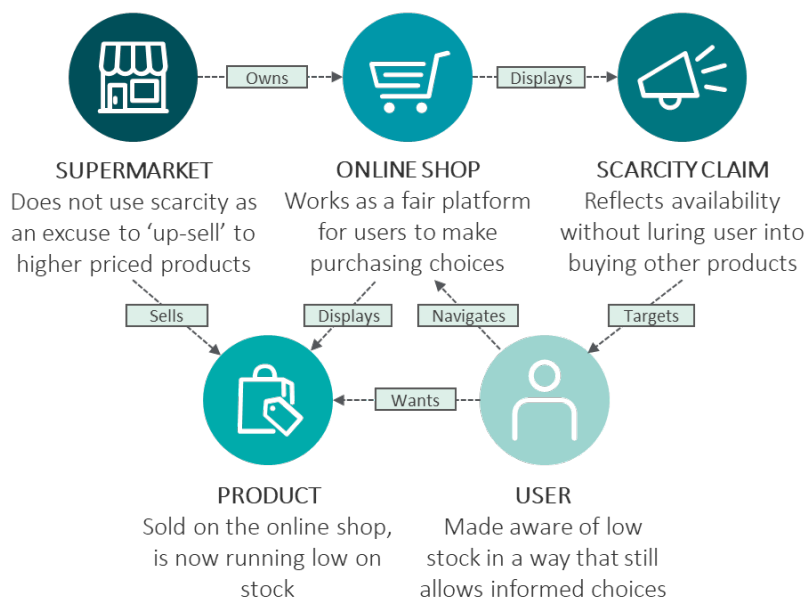
Timing: companies should assess the best time for presenting the relevant information about online traders so to maximise the possibility for users to take an informed decision (e.g., search results, product description, purchasing process, etc.).

Popularity claims: trader information should not be used by the platform provider as a popularity claim to mislead users (e.g., portraying it as a ‘quality guarantee’ for certain traders only).

Figure 4: online supermarket

Consumer protection from unfair trading regulations – regulation 5: traders are not allowed to use misleading actions to entice consumers to buy their goods or services (including providing false information on the availability of the product).

Supermarket chain selling products online without employing manipulative techniques to mislead customers’ decisions.



RELEVANT OCA AREAS

Scarcity claims: these claims can be misleading if they are used to steer consumers towards higher-priced products. They can also give a false impression that consumers must act fast to avoid missing out when this has no/limited bearing on the order the consumer may place.

Pricing: companies should avoid leveraging scarcity to manipulate prices. For example, Advertising a headline price only to add additional fees and charges later can be an unfair practice, especially where these are hardly avoidable or imposed based on high demand/low stock (drip pricing).

Framing: information should not be framed in a way that unfairly steers users towards a specific purchasing choice (e.g., up-selling).

Contacts



Suchitra Nair

Partner

snair@deloitte.co.uk

+44 20 7303 7963



Robert MacDougall

Director

rmacdougall@deloitte.co.uk

+44 20 7007 0148



Matteo Orta

Senior Consultant

morta@deloitte.co.uk






+44 20 8039 7554

The authors would like to thank Valeria Gallo, Ben Thornhill, Nick Seeber, Laurie Gilchrist, Brij Sharma, Anais Bauduin, Ahmed Hamdy, Mark Cankett, Barry Liddy and Mosche Orth for their contributions to this regulatory outlook.

Appendix 1: Digital Markets Areas*

*Please note - in practice AI capability will cut across a large number of these areas.







Connecting

-  Instant messaging
-  Social networks
-  Internet search
-  Internet and mobile gaming
-  Video calling/conferencing
-  Email newsletter platform







Content

-  Video sharing
-  Streaming video on demand
-  Streaming audio
-  News aggregators
-  Subscription services

Trading

-  Ad networks
-  Digital payments
-  Online marketplaces
-  Map platforms
-  Sharing and gig economy
-  Analysis of data

Enabling

-  Operating systems
-  App stores
-  Cloud computing
-  Internet browsers
-  Virtual assistants
-  Network connectivity

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London, EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.Deloitte.com/about to learn more about our global network of member firms.

© 2024 Deloitte LLP. All rights reserved.

Designed by CoRe Creative Services. RITM1646038