

Linklaters

Regulating the Digital Economy Series
Global Trends



Introduction

Regulation of the digital economy has become a priority for governments across the globe at a time when technology and data are more critical than ever.

The pandemic has accelerated our adoption of technology and we are ever more **dependent on digital services** to support our new ways of living and working. Technology will continue to have an important role to play in tackling the pandemic, for economic recovery and future growth.

There is, however, a concern that the **digital economy has been allowed to develop unchecked**, and that Big Tech has become too powerful, to the detriment of some businesses and consumers. There is increasing scrutiny of major technology platforms, their market power, use of personal data and responsibility for online harm.

There is a **wave of regulation and reform** which will shape digital markets: imposing more responsibility and greater liability on tech platforms, granting individuals more rights and protection mechanisms, and providing regulators with greater powers to intervene in both existing operations and the future expansion of businesses in the sector.

While regulators around the world are looking to address largely similar concerns, **their approach differs in major economies** such as the EU, the UK, China and the U.S..

The EU is pursuing a series of legislative initiatives intended to shape Europe's digital future and these are potentially a source of inspiration for regulation across the globe, in the way that the General Data Protection Regulation has been. The UK is also progressing ambitious plans as its position evolves post-Brexit. We are seeing the beginning of greater intervention in China and we could also see greater regulation and enforcement in the U.S..

Understanding how and **where regulators may intervene** is crucial to developing a coherent digital strategy in the markets where you operate.

“Momentum for change is building as lawmakers and regulators intervene in the digital economy.”

Clare Murray
Technology Strategy Consultant, London

Contents

This publication highlights the key issues we explored in our opening webinar in the Regulating Digital Economy Webinar Series and covers:



Part 1. The approach of some major economies



Part 2. Practical impacts of regulatory developments

Introduction

➔

Presenters

➔

1.1 European Union

➔

1.2 United Kingdom

➔

1.3 United States of America

➔

1.4 China

➔

2.1 Online harms

➔

2.2 Digital advertising

➔

2.3 Investment strategies

➔

Exploring the issues in more detail

We have dedicated publications on the topics which were the subject of subsequent webinars in the series:

- > Regulating the Digital Economy – [Payments Highlights](#)
- > Regulating the Digital Economy – [Digital Advertising Highlights](#)
- > Regulating the Digital Economy – [Online Harms: A comparative analysis](#)

For further insights on market developments visit [Linklaters – Tech Insights](#).

Part 1: The approach of some major economies

1.1 European Union leading the way

The EU continues to lead the way in the regulation of the digital economy, pursuing a series of legislative initiatives intended to shape Europe's digital future.

These ambitious proposals touch on almost every aspect of the digital economy: from ensuring well-functioning competition in digital markets to safeguarding users from online harms, establishing a framework for the regulation of Artificial Intelligence, and to improving operational resilience against a growing cyber threat.

The Brussels Effect

In the EU, the introduction of the General Data Protection Regulation (GDPR) was a watershed moment. This landmark piece of legislation regulates one of the core elements of the digital economy – (personal) data – and does so in an all-encompassing manner.




“The GDPR was something of a first globally. It has given rise to what is sometimes referred to as the ‘Brussels effect’, whereby EU regulatory initiatives may evolve to a de facto global standard and inspire regulation across the globe.”

Guillaume Couneson
TMT Partner, Brussels

By setting an EU standard for data protection, the EU took the first mover advantage. The GDPR has since been emulated by law makers in many other jurisdictions across the globe. We also see multinationals extending GDPR-style rights and protections across their operations as they seek to apply a common standard to their global IT systems and processes, usually implementing the strictest rules everywhere.

Europe's digital future – a complex matrix

The EU is now seeking to extend this regulatory approach to other areas of the digital economy. The new EU Commission has set out its ambitions to shape Europe's digital future. At a political level, the primary objectives are to rein in the power of online platforms and to better protect individuals as we spend more and more of our lives online. The priorities are:

-  1. technology that works for people;
-  2. a fair and competitive economy; and
-  3. an open, democratic, and sustainable society.

The diagram on the next page shows the breadth of the new legislation proposed for this “digital future”.

EU legislative process

Businesses should be aware that it is usual for draft laws to evolve through the legislative process, and to be prepared for the final product to be quite different to the first draft. They therefore need to keep on top of developments to be able to anticipate the measures they may need to take.

There is, however, an opportunity for key stakeholders to influence outcomes, by engaging in dialogue with the institutions on proposals as they go through the legislative process and to make any specific issues or concerns known.

EU Member States

In the meantime, a number of the EU member states are taking things into their own hands and their proposals will become law before European regulations are in force. They may influence the shape of the EU's approach to some extent and may create an additional level of complexity for business.



Learn more: [The EU and its decision-making process – why should you care?](#)

Germany at the forefront of reform

While there has been reform across various areas, a key focus in Germany has been reform of competition law. Germany became the first EU member state to bring in significant competition reform targeting tech, with the 10th amendment to competition law which came into force in January 2021.

The reform sets up a special regime for large tech companies under which the German competition authority can define a business as having “paramount significance”. Such a business will be automatically prohibited from certain conduct including self-preferencing, misuse of data and restricting interoperability. The law sets up a rebuttable presumption that this conduct harms competition. It also allows interim measures to be imposed more easily and quickly in digital markets.

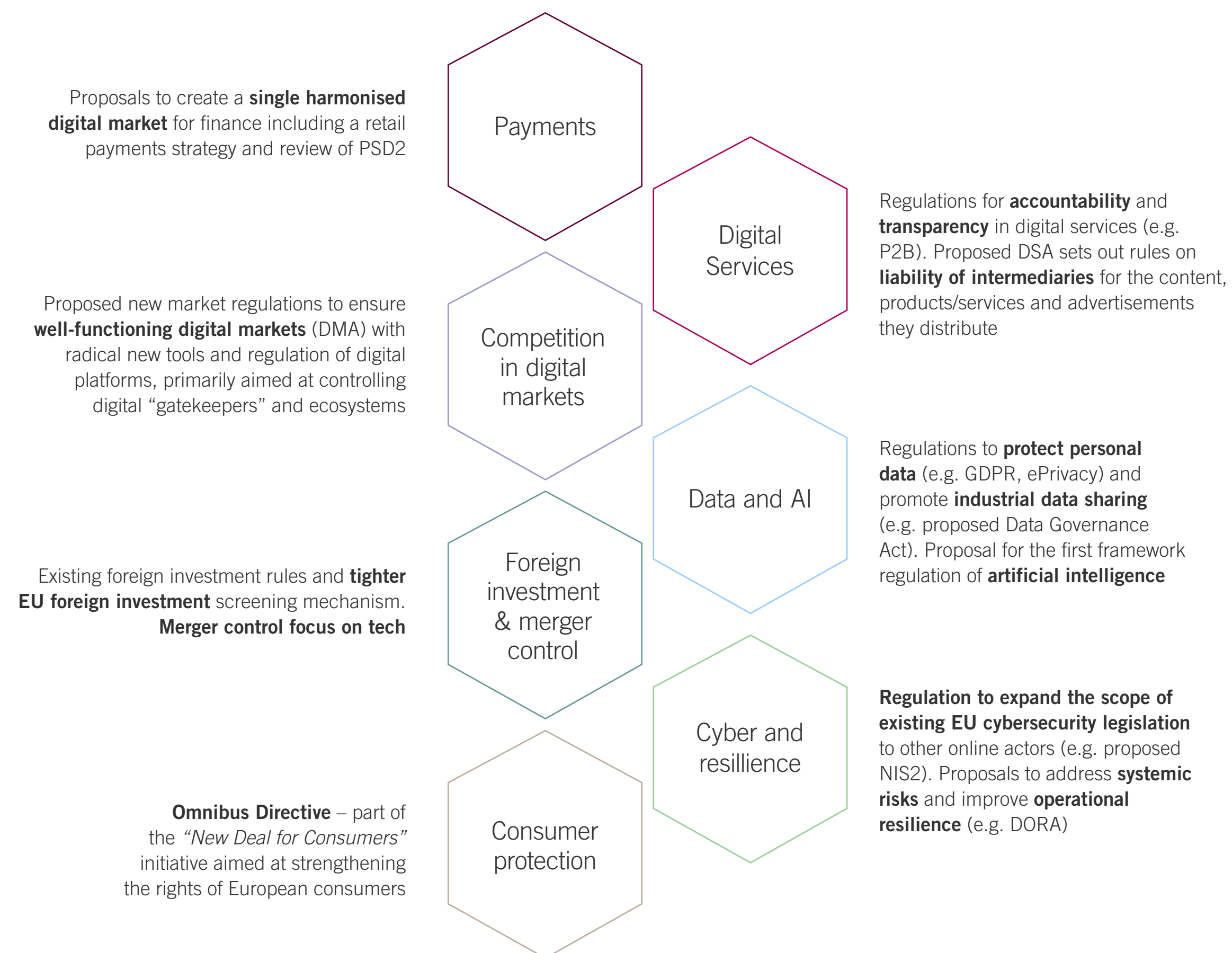
The concept of “paramount significance” is similar but not identical to the EU gatekeeper proposals under the Digital Markets Act.



Read more: [The revolutionary reform of German competition law – leading the pack in digital enforcement and other stories](#) (Jan 2021)

Part 1: The approach of some major economies

The EU digital regulatory matrix



Key impacts of EU proposals

Payments

The EU plans to create a single harmonised digital market for finance including proposed review of the regulatory landscape, hopefully with a view to greater harmonisation across the member states. This could **bring more tech companies and payments activity under the remit of financial regulators** but should also provide greater regulatory certainty and stability for the market.



Read more in our [Regulating the Digital Economy – Payments Highlights](#)

Intervention in competition in digital markets

There is increasing antitrust scrutiny of digital markets in the EU and individual EU member states. The EU’s proposed Digital Markets Act is intended to ensure well-functioning digital markets, with radical **new tools and regulation of digital platforms**, primarily aimed at controlling digital “gatekeepers” and “ecosystems”.

By regulating how digital gatekeepers can operate their ecosystems, deal with businesses active on their platforms and provide access to key inputs and IP rights, these rules could **impact all companies doing business in Europe’s digital economy**.



Read more: [The Digital Markets Act variations on the theme of competition policy](#) (Feb 2021)



Read more: [Five themes from the European Parliament’s first effort to reshape the EU’s Digital Markets Act](#) (June 2021)

Foreign investment and merger control

In developing investment strategies, consideration will need to be given to **foreign investment and merger control rules and the risk of regulatory intervention**. Tech and dynamic markets are a focus for merger control authorities and a hotspot for enforcement and policy review.

The EU and a number of member states have introduced tighter foreign investment controls including **new rules aiming to protect the tech sector**, and governments are using their tools to intervene more aggressively than ever before. These controls are resulting in record numbers of filings needing to be considered and deals subject to longer review processes. [See Section 2.3](#)

Part 1: The approach of some major economies

Consumer protection

As part of the EU Commission's "New Deal for Consumers" initiative the Omnibus Directive amends existing directives on Unfair Contract Terms, Price Indications, Unfair Commercial Practices and Consumer Rights. It seeks to make **consumer protection and certain rules on unfair competition practices, fit for the digital age**. Key to the approach will be enhanced enforcement measures, increased consumer rights and transparency compliance requirements – to be applied by member states by the end of May 2022.


Regulation of digital services

The EU's proposed Digital Services Act, if adopted as it stands, will set out rules on the liability of intermediaries for the content, products/services, and advertisements they distribute. *See Section 2.2*

 Read more: [Raising the bar – the European Parliament moves to toughen the Digital Services Act](#) (June 2021)

 Read more: [European Commission proposes impactful reform of rules for digital platforms](#) (Dec 2020)

The EU's proposed ePrivacy Regulation is intended to replace the ePrivacy Directive which was adopted in 2002 and later enhanced and extended. It contains **additional rules to align the ePrivacy rules with the GDPR** and addresses the use of cookies, email, and phone direct marketing, use of electronic communications content and metadata, etc.


 Read more: [EU: The ePrivacy Regulation – Let the trilogue begin!](#) (Feb 2021)

Increasing data regulatory enforcement

Data protection – With GDPR in force and data protection enforcement on the rise across the EU, use of personal data **is the subject of increasing scrutiny by data protection authorities**. One key area of regulatory focus is **the international transfer of personal data from the EU to third countries**. Following the Court of Justice of the European Union's decision in the *Schrems II* case, companies need to carefully assess whether their cross-border data flows comply with the requirements of the GDPR as interpreted by the Court.

 Read more: [EU – The EDPB's uncompromising new recommendation on transborder dataflow](#) (June 2021)


Data litigation risk – Claimant friendly developments could enable individuals to pursue **collective actions** for alleged privacy breaches more easily, creating an even tougher privacy regime and heightened litigation risk and costs.

 Read more: [European Union – Collective redress](#)

AI

The EU has proposed the first legal framework on AI (Artificial Intelligence Act) with prohibitions on the use of AI to the detriment of society and **onerous obligations for high risk AI systems**.


 Read more: [Regulatory superstructure proposed for artificial intelligence](#) (April 2021)

 Our [AI toolkit](#) provides guidance on how to deploy AI safely, ethically and lawfully.

Heightened cyber risk and regulation

The number of cyber attacks is on the rise and the ensuing disruption and the costs of dealing with cyber crises is growing substantially. Proposals have been tabled to expand the scope of existing EU cybersecurity legislation (NIS 2 Directive). This could mean **increased security requirements** (including supply chain security), more prescriptions for incident reporting as well as **more stringent supervisory measures** from supervisory authorities and stricter enforcement requirements.

Sector-specific regulation is also being introduced. For example, in financial services, the EU's proposed Digital Operational Resilience Act (DORA) is designed to address systemic risks and improve operational resilience. It is due to apply not only to financial institutions but also to some of their technology service providers.

 Read more: [Regulating the Digital Economy – Payments Highlights](#)




Part 1: The approach of some major economies

1.2 UK divergence after Brexit

In parallel to these EU developments, the UK is progressing its own initiatives covering the areas highlighted above in the EU regulatory matrix. While it is following similar principles to the EU, post-Brexit there is scope for divergence.

Digital Taskforce Advice

The UK's Competition and Markets Authority Digital Taskforce Advice published in December 2020, set out a bold proposal for a new regulatory regime for businesses with “strategic market status” (SMS). Like in Germany, the CMA would need to designate a business as having SMS. Once designated, the proposal is for a three pillar regime:

-  1. a code of conduct,
-  2. power to take pro-competitive interventions, and
-  3. a special merger clearance regime.



Read more: [A new regulatory regime for Big Tech: the CMA's Digital Taskforce Advice series](#) (Jan 2021)

Digital Markets Unit

The new regime is to be policed by a new Digital Markets Unit (DMU), which opened in April 2021. When the creation of the new unit was announced at the end of 2020, it looked as though the UK could become the **world leader in terms of a new regulatory regime for tech**. If the three pillar regime had been brought in, it would be. However, while the DMU is currently operating, it is only doing so in shadow form with no legal powers yet.

The timeframe for when the DMU will get powers is unclear – the latest announcements suggest early 2022. It is also unclear whether all three pillars will make it into law. It is a difficult issue in the context of Brexit and trans-Atlantic trade negotiations and some question if being a world leader in this area is really a good thing.

In the meantime, so far as the DMU is concerned, it is operating as more of a think tank and helping to shape proposed regulation with an ever-growing list of matters on its agenda.

“The UK, now out on its own, has made its own proposals which mirror aspects of each of the German and EU approach, but set their own tone.”

Verity Egerton-Doyle

Antitrust & Foreign Investment MA, London

CMA Investigations

While the DMU won't be able to take any enforcement measures, the CMA, within which the DMU sits, is using its existing competition law toolkit aggressively. The CMA has opened a number of investigations into platforms this year, with more said to be in the pipeline. However, a key issue is that the CMA can only use these competition law tools, and this really restricts what it can find to be a problem, and what it can do to fix it.

Broader UK tech regulation

Competition law and CMA enforcement offers one set of tools with which to address the issues of concern to the UK Government in relation to the development of the digital economy. The regulatory framework also includes the Information Commissioner's Office (ICO) in relation to privacy; and shortly, the Office of Communications (OfCom), on the forthcoming online safety regime.

This creates a **complex regulatory patchwork** that presents significant challenges for business – not least as the different branches of regulation do not always point in the same direction. This can make compliance a key challenge for tech companies: in the absence of a coherent and holistic regulatory framework, the burden of navigating the various areas of regulation sits squarely with businesses.

But there is some hope in the form of the **Digital Regulation Cooperation Forum** which was formed in July last year, with the UK's CMA, ICO and Ofcom – and as of April 2021, the FCA. The DRCF is a cooperation forum rather than a regulator with cross-cutting powers or objectives. However, the enhanced collaboration and cooperation it promises is a much-needed development, and a step on the difficult path towards a coherent regulatory regime for the digital sector.



Read more: [A step towards the pipe dream: UK regulators promise closer cooperation on tech](#) (March 2021)

Part 1: The approach of some major economies

1.3 Revamping the U.S. approach

While European jurisdictions are well developed in their approach to digital markets, the U.S. initiatives are at an earlier stage of development.

Increasing antitrust enforcement

During President Trump's administration we saw a particular focus on traditional antitrust and consumer protection enforcement with, for example, active enforcement of merger control across a range of digital markets and not just large platforms. In particular, we saw enforcement around deals that concerned nascent competitors, so-called "killer acquisition".

The federal agency also brought some landmark antitrust and consumer protection cases focused on alleged exclusionary conduct. It sought to unwind some major acquisitions, and in the view of the regulators, effectively prompted some of the platforms to reintroduce competition.

Foreign investment

We also saw foreign investment become a key priority with expanding CFIUS powers and some targeted legislation mainly around investments from China.



Read more: [Navigating CFIUS – A series](#)

Biden administration

Since the presidential election in 2020, all eyes are on Washington to see what tack the Biden administration will take and what role the new Congress will take. The White House has signalled that digital markets are a priority, and this is seen in some of their policy appointments including academic Tim Wu.

On the enforcement side Lina Khan, a progressive candidate, has been appointed as chair of the FTC, one of the key roles which will drive decision making in the U.S..

Private litigation

In parallel, we saw individual U.S. states and private litigants take action, seeking a more interventionist approach than that of the federal enforcers. This has added to some of the uncertainty in the enforcement environment in the U.S..

Antitrust legislation

We expect legislative developments in the U.S. where we have so far seen a patchwork of early stage Federal and State initiatives.

On the competition side, many authorities have focused on facilitating antitrust enforcement and reducing barriers to bringing cases. Congress is also trying to take a proactive approach to competition policy, holding

hearings to develop targeted legislation (including in digital advertising and app stores). The results of those initiatives are still developing.



Read more: [Antitrust complaint against Amazon highlights patchwork approach to US tech enforcement](#) (May 2021)

Online content

We are also seeing some bipartisan efforts which began under the Department of Justice in 2020, to revamp online harms, content moderation and Section 230 of the U.S. Communications Decency Act (immunity for liability).

While it is a bipartisan effort, there are some starkly conflicting priorities. We have seen increasing engagement with the platforms on what the right approach is, and we expect further developments in this area.



Read more: [Online Harms: A comparative analysis – U.S. section](#)

Data privacy

On the data privacy side, we have also seen a growth of new State regulations that are pushing a renewed focus at the federal level on data privacy regulation. The States are currently seen to be the long pole that is driving the broader policy in the U.S. with the California Privacy Rights Act and the Virginia Consumer Data Protection Act both coming into effect in January 2023.

The FTC has signalled that if federal legislation is not forthcoming, they may take a more proactive consumer protection role. Overall, there is a lot in the works in the U.S. in the early stages of development and we expect to see more in the coming months.



Read more: [Virginia enacts comprehensive privacy legislation](#) (March 2021)

Part 1: The approach of some major economies

1.4 China's response to global developments

China's digital economy is a vast market with 900 million internet users, four million distinct websites and three million mobile apps. Its recent approach to the digital economy has been shaped by the U.S.-China tech rivalry and action taken by the U.S. – such as President Trump's executive orders against WeChat and TikTok in summer 2020 – which has motivated China to make its digital economy and tech generally more self-sufficient.



Read more: [Tick tock, tick tock: Trump's headache-inducing executive order aimed at WeChat](#)

Five Year Plan

The Beijing legislature held two key meetings in March this year and it is very clear from the new Five Year Plan that came out of those meetings that the digital economy will be at the centre of driving the economy in a post pandemic world.

The regulations and policies giving effect to the new Five Year Plan are designed to further the objective of self-sufficiency with more investment in 5G, AI and semiconductors.



Read more: [Read more: 2 + 5 = Tech!](#)

Foreign investment environment – a regulatory balancing act

There are lots of opportunities for businesses coming to market but, for Chinese regulators, there is a fine balancing act. Promoting innovation is key to driving the economy after Covid-19. However, regulators want to make sure that we do not get to the stage we saw around the world in the 2007/08 financial crises where companies were too big to fail.

Scrutiny of China Big Tech

Numerous regulations have been introduced in 2021 in China. There has been scrutiny of consumer finance platforms and the largest ever fine from the Chinese antitrust regulator was seen in April. These developments are aimed at ensuring the digital economy is stable and that from a societal perspective, consumers believe that they have more protection. Stability in society is considered key to allowing China's economy to grow in a sustainable manner.



Read more: [China's SAMR joins ranks and sends a strong signal for digital markets](#) (Jan 2021)

More enforcement powers

In addition, the new regulations give regulators more enforcement powers. We have seen a lot of focus on antitrust across the tech and fintech ecosystems. Thirty-four of the leading tech companies have been in meetings with regulators. The regulators are looking at how these giant platform players arguably have a dominant position in their markets and sub-markets.



Learn more: [Tech Investment and Operational Landscape in China \(webinar\)](#) (Spring 2021)

Data management and security

In terms of data management and data security, in the last 12-18 months there has been a real enhancement in enforcement and scrutiny of companies. China is one of the jurisdictions in Asia that has really taken the GDPR and brought it into the local regime to enhance the protections for consumers and the compliance requirements on companies. This will be further reinforced through the new personal information protection law expected soon and data compliance is a tool that the Chinese government will use to stabilise the digital economy.



Read more: [Third time \(un\)lucky? China finalises its Data Security Law](#) (June 2021)

[“Security of digital markets is set to increase in China, where enforcement of domestic tech players has previously been more light touch than elsewhere.”](#)

Alex Roberts
TMT Counsel, Shanghai

Part 2: Practical impacts of regulatory developments

2.1 Online harms

One of the key areas of regulatory focus is tackling harmful content online, so-called “online harms”. This covers both **clearly illegal material** (such as terrorist content) and material that is **lawful but harmful** (such as disinformation about vaccines).

Previously, online platforms were subject to a **patchwork of discrete laws on particular topics** and voluntary initiatives in this area. Now governments are looking to replace this with more holistic regulation for those who host content or allow users to interact with one another. The pace of change is rapid with new regimes being proposed or coming into effect in many jurisdictions.

“The challenge for lawmakers is to balance the desire to reduce the risk of harm against the need to respect fundamental human rights.”

Ben Packer

Dispute Resolution Partner, London

In considering regimes across the globe, we looked in detail at the current legal position in Australia, France, Germany, Singapore and the United States and we looked ahead to the ambitious proposals in the EU, Ireland, and the UK. From our analysis we have identified five key themes:

1. Organisations in scope

There is a broad **range of intermediaries in scope**. For the jurisdictions we focused on in our publication, all the regimes applied to **social media, cloud hosting sites and video content platforms**. Some regimes also covered **video games, online marketplaces, and search engines** and some, like those in Australia and Singapore, and those proposed in the UK and Ireland, also cover private communications or user to user interactions.

2. Types of harm

There is *some* consensus of the **types of harms** that users need to be protected from. All the regimes we looked at imposed obligations on platforms in respect of **illegal content** – such as content promoting terrorism or CSA material. However, some regimes go beyond this and expect *certain* platforms to take action in respect of content that is lawful but harmful.

3. Nature of obligations

The obligations on platforms can be divided into two camps. Some regimes – for example Germany, Australia, and Singapore – frame obligations in terms of **individual pieces of content**: “once you are notified, you must take down this type of content within this period of time”. Other regimes – for example the EU, Irish and UK proposals – frame the obligation in terms of the overall **systems and processes platforms** must have in place to mitigate the risk of harm. Typically, this requires firms to conduct a form of risk assessment and then design measures to mitigate the risk of harm occurring.

While there are fundamental differences in how the overarching obligations are framed, there are **some common obligations across regimes**: for instance, many if not all of the regimes impose obligations to block or remove certain types of content, to provide user reporting mechanisms and to publish transparency reports on the types and volumes of content removed.

4. Sanctions

Virtually all the regimes do or will provide authorities with pretty **meaty powers to sanction non-compliance** – including fines, criminal liability and even, as a last resort, requiring ISPs to block access to non-compliant platforms.

5. A fast-moving area

There are regulatory regimes in force in certain jurisdictions already but the **most ambitious are still being developed and debated** – for instance, the proposals in the EU, the UK and Ireland.

Practical impact of evolving online harm regimes

Businesses will face a significant challenge in implementing frameworks that allow the platform to comply with each regime – while maintaining a consistent user experience. Platforms will need to make choices about whether they decide to take the highest regulatory standard and apply this globally – or differentiate country-by-country.

This challenge will be made harder still by the fact that these regimes will not impose consistent obligations. There will be areas of divergence and possibly even opposing obligations in different jurisdictions.

Furthermore, in designing their systems and processes, platforms will have to think about more than just the online harms regimes. They will also need to consider other regulatory and legal obligations, such as data privacy and competition law.

There is still some uncertainty in exactly what these proposals will look like in their final form, but one thing is certain: this is going to be an area of growing significance for ever-more online businesses in the coming years.



Read more in our global thought leadership: [Online Harms: A comparative analysis](#)



Read more: [Draft UK Online Safety Bill published](#) (May 2021)

Part 2: Practical impacts of regulatory developments

2.2 Digital advertising

Digital advertising is one of the markets that has so far attracted the most attention for lawmakers and regulators. It is also an area in which the issues raised by siloed regulation are perhaps most stark, due to the differences between competitive and privacy imperatives.

The competition problem and how to fix it

From a competition perspective, the fundamental “competition problem” which the authorities identify is a classic one: the **market power of the largest social media platforms** at various levels of the AdTech stack. If we are thinking of our competition toolkit, we have two issues:

- > **First** – competition law does not prohibit dominance; it prohibits abuse of dominance. **Establishing abuse is notoriously difficult**, requiring proof of conduct which either excludes competitors or exploits customers. There are some cases on foot now – including litigation in the U.S. – seeking to establish this, but no infringement findings yet.
- > **Second** – and even more significantly, is **how to “fix” the problem**. This is where interactions and indeed tensions with privacy come in. Given that the source of the market power is the data held by Google and Facebook, the natural “competition”-based solution would be to force that data to be made available to competitors, which could raise privacy concerns.

As long ago as 2016, the French and German authorities co-authored a report on Big Data in which they concluded – for these and other reasons – that a **case-by-case approach** is necessary. The CMA’s digital advertising market study which concluded in July 2020 came up with various potential solutions, including compelling Google to provide access to the

data underpinning its search algorithm, unbundling Google’s role at different levels of the AdTech “stack” and proposals for interoperability and the creation of a “secure common digital ID”. Any and certainly all of these together would fundamentally change the landscape of digital advertising.

The third party cookie

One particular area of focus has been changes to the third-party cookie. Apple has already phased out third-party cookies on Safari and privacy regulators have put Google and to a lesser extent, Facebook under pressure to improve privacy for users. However, Google’s proposed privacy sandbox is currently under investigation by the CMA after a complaint by publishers that the step would decimate their advertising revenues.

The CMA has said it is working with its new Digital Regulation Cooperation Forum on this case, which includes the ICO, but it is difficult to see how the problem can be solved with the competition toolkit alone.

This raises the obvious question of whether a more **fundamental regulatory solution** is needed. From a UK perspective, if the newly established DMU does ultimately get the power the CMA has requested to issue “pro-competitive interventions”, it could make the changes suggested by the digital advertising market

study. At an EU level however, a more institutional framework is on the table through the combination of the Digital Markets Act, the Digital Services Act, and the Data Governance Act.

The data protection perspective

The key objective of the GDPR is protecting personal data, in particular by **restricting data processing**. Numerous provisions of the GDPR prevent processing (e.g. data minimisation, purpose limitation, storage limitation, need for a legal ground and the concept of compatibility). Data sharing under GDPR is not impossible, but it is heavily conditioned. Personal data is not an “asset” that can be traded in the traditional sense: companies need to keep the individual to whom the personal data belongs at the centre.

Contradictions between data protection law and competition law

Data protection legislation is trying to achieve very different objectives compared to competition law and therefore it can appear contradictory and difficult to reconcile at times. For example, Apple’s decision to no longer allow tracking by apps without consent will appear positive from a data protection perspective, while it could raise questions from a competition law point of view.

Part 2: Practical impacts of regulatory developments

Digital advertising and the Digital Services Act and the Digital Markets Act

As the EU is diving deeper into the regulation of cyberspace, the question of data (including personal data) is at the centre of many of the concerns. Looking specifically at digital advertising, we see it is given attention under both the DSA and the DMA, which address **the need for transparency**.

The DMA's transparency obligations are towards publishers/advertisers while the DSA imposes obligations to, for example, maintain a database of displayed ads which may be very valuable, especially when combined with the purchase history of an individual to track the efficiency of advertisement.

Article 36 of the DSA provides that the European Commission will facilitate the drawing up of EU level **codes of conduct** between platforms and other service providers in online advertising and provides that these must be drawn up in accordance with both competition and data protection laws.

Reconciling regulatory objectives – the Data Governance Act

A tentative solution to regulatory reconciliation has been tabled by the European Commission through the proposed Data Governance Act (DGA). The DGA addresses a broad range of topics, but from a digital advertising perspective the most notable feature is that it sets out a **framework for establishing a new type of data intermediaries**. These intermediaries would be not for profit organisations that would enable companies to share data (potentially including personal data) with others, without the recipient having full access thereto.

This proposal has received a mixed reaction. In a joint opinion on the proposed DGA, two EU-level bodies in charge of data protection consider that, on the one hand, the proposal says that it is without prejudice to the GDPR and does not aim to change this piece of legislation while, on the other, it is proposing certain principles that are fundamentally irreconcilable with the GDPR. How this feedback will be taken into account by the EU legislators and whether the data sharing mechanisms proposed by the DGA provide an avenue for AdTech remains to be seen.

Future developments

We expect digital advertising to continue to be the focus of lawmakers and regulators in the coming months, particularly in the U.S. and Europe. We explore this in more detail in our third webinar.



Read more: [Regulating the Digital Economy – Digital Advertising Highlights](#)

“Reconciling competition and data protection objectives will be key to proper digital regulation. However, the recipe still has to be invented.”

Guillaume Couneson
TMT Partner, Brussels

Part 2: Practical impacts of regulatory developments

2.3 Investment strategies

It is clear that the enforcement environment in digital markets has had a very significant impact on investments and M&A activities. Jurisdictions around the world are expanding their enforcement authority and introducing greater risk for transactions. There are some key themes for tech companies to focus on.

“Businesses will need to carefully manage the timing and completion of deals and the risks around the underlying certainty. The need for early deal planning is more critical than ever.”

Alex Roberts
TMT Counsel, Shanghai

Tightening of merger control review and more aggressive enforcement

Authorities have been concerned that historic “underenforcement” in dynamic markets relating to (primarily the U.S.) Big Tech mergers, has helped to create or cement (primarily U.S.) Big Tech monopolies.

Authorities are grappling with how to deal with dynamic markets and whether “traditional” merger control is still fit for purpose. Many authorities feel that **tech deals have slipped through the merger control net**, particularly through “killer acquisitions” by Big Tech.

The result is that enforcers around the world have sought to do a number of things to ramp up their enforcement in tech mergers. Firstly, they have **expanded reporting rules** to require approval for more transactions, particularly shifting the focus to deal values in countries like Germany or proposing sector specific notification rules as they are doing in Australia.

There is currently reform at the EC level where revised **guidelines will allow the EU to review deals** that don’t meet the threshold tests at member state level. The UK’s Competition and Markets Authority also uses its elastic jurisdictional thresholds and “share of supply test” as a gateway to review transactions that it considers interesting.

There is also less certainty around deals that do not have mandatory reporting requirements so there are more non-reportable deals that are being challenged and we see that both in the EU’s expansion of its deferral rules recently but also in the enforcement in the U.S. which seeks to unwind deals that have closed despite approval.

We are also seeing **more aggressive enforcement in challenging deals** particularly those involving actual or potential competitors and that’s not just in deals by the large tech platforms. It is also for other companies who are acquiring start-ups and others that may be seen as disruptive.

We are also seeing some unexpected geographic focus where the UK, for example, has blocked deals with only a very limited nexus to the UK and where the focus of the deal is really another jurisdiction like the U.S..



Learn more: [Summer’s Top Antitrust & Foreign Investment Stories 2021 – Rigorous but uncertain global merger control enforcement](#) (June 2021)

“The EU is gearing up to call-in and review non-notifiable deals, bringing it in line with other major regimes but with fewer safety valves and tech deals in focus.”

Verity Egerton-Doyle
Antitrust & Foreign Investment MA, London

Part 2: Practical impacts of regulatory developments

Increasing significance of foreign investment controls

Foreign investment is another area where we are seeing substantially greater risk, particularly as countries seek to protect their domestic industries following the pandemic.

“The expansion of foreign investment rules and uptick in notifications show no signs of abating. This has resulted in a substantial ramp-up in reporting requirements, particularly in jurisdictions across Europe.”

John Eichlin

Antitrust & Foreign Investment Counsel, New York

We are also seeing much lower thresholds in countries such as Australia which have, in some cases, removed them entirely and we have seen a greater focus on critical technology and data. All of this is introducing timing and transparency risks, particularly in the new regimes where practice is less established.



Learn more: [Summer's Top Antitrust & Foreign Investment Stories 2021 – Increasing and unpredictable](#)



Read more: [Foreign investment controls by jurisdiction](#)

Impact on corporate structuring and governance issues for boards

The regulatory developments referenced above are really making boardrooms now sit up and think about their corporate and governance structuring and we are working with multinationals that recognise that changes may be required for the long-term sustainability of their operations across the globe.

Chinese domiciled multinationals are also contemplating the U.S.-China tech rivalry, the U.S. administration's policies against China headquartered tech companies last summer and uncertainty as to the approach of the Biden administration.

Chinese domiciled multinationals are thinking about what they need for their rest of the world business. They are considering whether they need to disassociate themselves with the China mainland and to set up, for instance, an alternative overseas headquarters or, as we saw with Oracle and TikTok, the overseas or U.S. business bringing in non-Chinese management.

Alternatively, they may consider segregating the business in terms of data quarantine, information barriers or other separation measures which, on a long-term basis, will allow businesses to continue to operate cross-border.



Read more: [Tech Legal Outlook 2021: Shifting global dynamics](#)

Presenters

**Clare Murray**

Technology Strategy Consultant,
London

Tel: +44 20 7456 2126
clare.murray@linklaters.com

**John Eichlin**

Antitrust & Foreign Investment Counsel,
New York

Tel: +1 21 2903 9231
john.eichlin@linklaters.com

**Guillaume Couneson**

TMT Partner,
Brussels

Tel: +32 25 01 9305
guillaume.couneson@linklaters.com

**Alex Roberts**

Corporate & TMT Counsel,
Shanghai

Tel: +86 21 2891 1842
alex.roberts@linklaters.com

**Verity Egerton-Doyle**

Antitrust & Foreign Investment
Managing Associate, London

Tel: +44 20 7456 3389
verity.egerton-doyle@linklaters.com

**Ben Packer**

Dispute Resolution Partner,
London

Tel: +44 20 7456 2774
ben.packer@linklaters.com

linklaters.com

This publication 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 or on other areas of law, please contact one of your regular contacts, or contact the editors.

© Linklaters LLP. All Rights reserved 2021

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 Linklaters 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, One Silk Street, London EC2Y 8HQ, England or on www.linklaters.com and such persons are either solicitors, registered foreign lawyers or European lawyers.

Please refer to www.linklaters.com/regulation for important information on our regulatory position.