10 Global Digital Markets Regulatory Issues To Watch

By **Francesco Liberatore and James Konidaris** (February 8, 2021)

Francesco Liberatore

James Konidaris

Developments in digital markets regulation show no signs of slowing down in 2021. The sector has experienced an accelerated growth and acquired reinvigorated strategic importance throughout the historic global pandemic of 2020.

With more vigorous enforcement, a number of significant policy reviews and broader political movements, such as the end of the transition period in the U.K.'s exit from the EU and the new Biden administration in the U.S., there are plenty of regulatory developments impacting the industry in the year ahead. International businesses will want to keep a close eye on the following developments in 2021 given their impact on operations globally.

1. The Rise of Global Digital Markets Regulations

Digital markets potentially face new regulation across the world to deliver greater competition and innovation for the use of data, while protecting consumers' rights. However, these proposals come with controversy.

For example, in the EU, the European Commission has made two ambitious proposals.

The proposal for a new Digital Services Act will replace and expand the 2000 e-commerce directive and aims to harmonize the conditions that determine the responsibilities and liability regime for online intermediary services, notably large online platforms.

The proposal for a Digital Markets Act introduces a new competition regime for online platforms acting as gatekeepers in digital markets. These proposals represent a watershed moment for Ursula von der Leyen's commission, which has made so-called technological sovereignty, or efforts to bolster the bloc's role in digital markets, a central piece of its legislative agenda.

However, both proposals are expected to undergo significant amendments before the European Parliament and Council to reconcile their aims with general EU law principles of regulatory forbearance, effectiveness and proportionality.

These proposals are not alone on the global stage. Similar proposals have been tabled in the U.K., with the creation of a digital markets unit within the Competition and Markets Authority and a new regulatory regime for digital markets players with strategic market status and Australia.

In the U.S., legislators issued a much-anticipated report on competition in digital markets that calls for major antitrust reforms. The new Biden administration is expected to take a firmer stance on antitrust enforcement — particularly with respect to nascent competition — potentially aligning the U.S. more closely with Europe.

In China, the authority is working on guidelines to clarify how anti-monopoly rules apply to platform conduct; and regulators in Japan plan to begin monitoring certain platforms

through mandatory disclosures of certain business practices.

Given the cross-border nature of digital markets, the Organization for Economic Cooperation and Development has noted, "Governments may need to enhance co-operation across national competent agencies to address competition issues that are increasingly transnational in scope or involve global firms."

2. Regulation of New Digital Communications

The continuing evolution and advancement of digital communications around the world, from software-defined networking in a wide area network to over-the-top media services, has created significant business opportunities and advantages across borders.

In response to such evolution and advancement, regulators around the world are reviewing their existing telecom regulation to see if it still fit for purpose in this converging digital environment. The EU is leading the charge this time, with a recast of the regulatory framework for electronic communications applicable throughout the European Economic Area through the adoption of a new EU Electronic Communications Code, which member states had to transpose into national law by, and apply from, Dec. 20, 2020.

The code attaches different regulatory treatment to different categories of regulated networks and services, for example, private networks are subject to lighter regulation than public networks, and number-independent services are subject to lighter regulation than number-dependent services (i.e., services allowing a dial-in or dial-out functionality with national or international numbers).

The extent to which the regulation will apply to new forms of digital communication, as well as the actual obligations applicable to each network and service, will, therefore, depend on its legal characterization under the code. While the majority of member states are late in transposing the code, partially due to the pandemic, EU case law requires them to apply existing rules in a manner that would not compromise the application of the code even prior to its transposition.

Despite the U.K.'s exit from the EU, the U.K. government has pledged to apply the code in the U.K. too, but has so far delayed the extension of the rules to number-independent services. This might well change in 2021.

Elsewhere, several other jurisdictions outside the EU are looking to review their current regulatory approach to bring it in line with the new definitions contained in the code, which makes it an international gold standard for the regulation of new communications services and networks. Therefore, ensuring compliance with the code will be a key theme for 2021.

3. Network Sharing and Co-Investment in Digital Infrastructure

Another change introduced by the code is the promotion of network sharing and co-investment in new very high capacity networks to reduce costs and increase efficiencies in rolling out new 5G, fiber and other gigabit-capable networks.

However, in some circumstances, this cooperation may have a negative impact on competition. As a general rule, arrangements to share passive infrastructure (ducts, poles, power, dark fiber, etc.) in rural areas tend to be seen more favorably than active network sharing arrangements.

Similarly, open co-investment arrangements are seen more favorably than exclusive arrangements. However, each must be assessed on its own merits. Therefore, competition authorities may also be prepared to approve more extensive network sharing and exclusive co-investment arrangements subject to commitments and safeguards to disentangle the pro-competitive aspects of the cooperation from its anti-competitive effects.

A recent successful example of this trade off is the commission's approval of the Infrastrutture Wireless Italiane SpA, or Inwit, joint venture in Italy last year, subject to certain commitments from the joint venture parties. Finally, the commission has consistently maintained that network sharing may be a less restrictive alternative to mobile mergers, even when those mergers do not lead to or strengthen a dominant position, often called merger gap cases.

Last year's judgment by the EU General Court in CK Telecoms U.K. Investments Ltd. v. European Commission, annulling the commission's prohibition of a U.K. mobile merger, if upheld by the EU Court of Justice, might change this perception in 2021 and, some commentators say, might spur new attempts of consolidation in the mobile sector.

4. End-to-End Encryption

The possibility to impose EU obligations to messaging services using end-to-end encryption to cooperate with law enforcement agencies has been dominating justice and home affairs discussions for some time now, as a way to better prepare for planned terrorist attacks throughout Europe.

A council of home affairs ministers endorsed on Dec. 14, 2020 a council resolution on encryption, paving the way to create a regulatory framework to that effect in 2021. Since 2015, a series of campaigns run alternately by Europol and the Federal Bureau of Investigation, or the services of the Five Eyes alliance, were building towards the development of this council resolution.

In October, interior ministers of the alliance called on the internet companies, once again, to equip their IT networks with backdoors so that law enforcement agencies and competent authorities could access end-to-end encrypted apps to police online criminality.

The resolution in itself is unlikely to lead rapidly to a move for new EU regulation in this area, but action at national level, justified by the national security exemption in the code, may be contemplated. The broad range of consequences to the tech sector stemming from the resolution should be closely monitored and assessed.

5. Foreign Direct Investment Controls and Impact on M&A

Despite the 2020 pandemic, mergers and acquisitions in telecom, media and technology markets continues to account for the largest share of global M&A transactions by value and volume. The 2020 global pandemic and the resulting economic crisis, however, resulted in the tightening of existing, or spurred the adoption of new, foreign direct investment control regimes across the world, which is likely to render deal making in this sector more complicated.

For example, in the EU, the screening regulation has established a mechanism of cooperation and coordination of national screening procedures for new foreign direct investment s that are maintained by member states.

However, the screening regulation does not replace member states' screening mechanisms and confirms the ultimate power of member states to admit or introduce restrictions/conditions for new investments. Therefore, the expansion of national foreign direct investment regimes carries the inevitable risk of a resurgence of national protectionism and raises the need to factor in political risk in deal planning in 2021.

One of the most notable new foreign direct investment regimes outside the EU is the U.K.'s National Security Investment Bill, which is currently before the House of Lords for debate and approval. Under this new regime, certain direct foreign investments, as well as domestic transactions, in the U.K. would require mandatory notification to, and prior approval by, the Department for Business, Energy and Industrial Strategy before completion.

In addition, the department will be able to call in retroactively deals — within six months of becoming aware of them — that fall outside the mandatory notification requirements, but which it deems still to raise potential national security risks. The Department for Business, Energy and Industrial Strategy will be able to look backwards at deals that closed within five years, so long as they closed on or after Nov. 12, 2020.

Sectors falling within the National Security Investment Bill regime include communications, satellite and data infrastructure. The government estimates that the new regime would be likely to lead to between 290 and 860 notifications of trigger events per year, and between 70 and 95 call-ins per year. Of these, around 10 per year are thought likely to require remedies.

6. Net Neutrality Regulation Brings Questions

While net neutrality rules might make a comeback in the U.S. under the Biden administration, on the other side of the Atlantic, all eyes are on the application of the new Body of the European Regulators of Electronic Communications guidelines for the regulation of the EU's net neutrality rules, which were adopted in mid-2020. The rules prohibit blocking, throttling or discrimination of online content, applications and services.

However, some operators continue to test the boundaries of these rules, in particular in connection with zero rating and traffic management measures. Last year, the EU Court of Justice interpreted the EU net neutrality rules for the first time and found that:
The requirements to protect internet users' rights and to treat traffic in a non-discriminatory manner preclude an internet access provider from favouring certain applications and services by means of packages enabling those applications and services to benefit from a 'zero tariff' and making the use of the other applications and services subject to measures blocking or slowing down traffic.

However, many questions remain unanswered as a matter of law, including whether certain services are caught by the regulation at all or are exempted as specialized services.

This is, for example, the case with in-flight connectivity. Prior to the U.S. Federal Communications Commission's decision to repeal the net neutrality rules altogether in December 2017, in-flight connectivity service offerings were exempted from the FCC rules just like other ancillary offerings of connectivity on premises, such as internet cafés.

The FCC considered that open and transparent offerings of limited connectivity services that are less than full internet access or that are not mass market retail services — as it is the case with in-flight connectivity — were not subject to the FCC's net neutrality rules at all.

By contrast, last year, the Body of the European Regulators of Electronic Communications rejected the notion that in-flight connectivity is exempted from the EU net neutrality rules. As the aviation sector starts recovering from the global pandemic, it remains to be seen if the BEREC decision might pose a regulatory obstacle to the growth of the EU in-flight connectivity market.

7. Recovery and Resilience Facility and State Aid for Digital Markets

The Recovery and Resilience Facility is an ambitious instrument that will be at the center of the recovery of the EU economy in 2021, through the provision of €750 billion to support financing in the EU's 27 member states.

The Recovery and Resilience Facility will support medium- to longer-term reforms and investments, notably in green and gigabit-capable technologies, such as 5G and fiber, with a sustainable and lasting impact on the productivity and economic and social resilience of the applicant member states.

The commission already earmarked 20% of the recovery cash for initiatives that make their economies more digital. In this area, these reforms and investments include notably 5G coverage, large-scale deployment of 5G corridors along transport pathways, ubiquitous access to ultrafast connectivity in urban and rural areas and affordable to all households and businesses, and connecting all socioeconomic drivers to very high-capacity broadband networks.

Key aspects of the application of the Recovery and Resilience Facility will be accountability and compliance with state aid rules. Union funds channeled through the authorities of member states become state resources and can constitute state aid. Therefore, state aid rules fully apply to the measures funded by the Recovery and Resilience Facility.

As a rule, state aid measures must be notified to, and cleared by, the European Commission before funds are granted, unless they comply with the conditions of the applicable General Block Exemption Regulation declaring certain categories of aid compatible with the internal market. The onus is on both the state and the aid recipient to satisfy themselves that the state aid is compatible because it is approved or exempted.

To assist with the application of state aid law to the broadband projects sponsored by the Recovery and Resilience Facility, the commission is currently reviewing its state aid framework for broadband projects — this review is expected to be completed in 2021 — and has published additional guiding templates for granting authorities and potential beneficiaries.

Based on this guidance, state aid for rural areas and incentivizing a step change in technology are seen more favorably than aid in more competitive areas. However, there may be instances where the benefits of the state aid even in the more competitive areas, in terms of having an incentive effect or the promotion of services of general interest, may outweigh the potential risk of crowding out private investment, and thus be permissible.

8. E-Commerce and Pricing Algorithms

Another effect of the 2020 pandemic is that consumers redirected their purchasing and spending to online sales. For example, in the EU, online sales reportedly grew by 30%-40% after lockdown restrictions were introduced in March last year. This trend shone a light on

certain online sale practices that raised concerns for competition and consumer protection authorities, concerning geo-blocking, resale price maintenance, price gauging and the use of pricing algorithms, among other issues.

Some commentators questioned whether existing competition and consumer protection rules are well equipped to deal with such concerns. These questions spurred a rethink of the existing approach to enforcement on e-commerce.

For example, the European Commission is revising its competition rules on vertical distribution agreements with a view to ensuring that the rules are fit for purpose in digital markets.

The Italian Competition Authority is investigating the terms and conditions of global leading providers of cloud computing services, focusing in particular on allegedly improper collection of user data for commercial purposes; undue influence on consumers; and failure to provide consumers with information on their right to withdraw from the contract and/or to access alternative dispute resolution — interestingly, the Italian Competition Authority's approach seems to echo enhanced sector-specific consumer protection provisions contained in the code.

More recently, the U.K. Competition and Markets Authority established a data, technology and analytics unit studying new tools to tackle potentially anti-competitive uses of pricing algorithms, and launched a public consultation on how algorithms can harm consumers.

One of the most contested theories of harm is tacit collusion between self-learning algorithms. It is settled case law that competitors can intelligently adapt to the market without infringing antitrust law, as long as there is no concurrence of wills between them, replacing independent decision making with collusion.

However, it is an open question whether self-learning algorithms that signal prices to each other and learn to follow the price leader would fall within this safe harbor. There is no precedent to date on this latter scenario, but the EU case law on price signaling may provide a useful analytical framework.

Based on this case law, businesses may arguably need to ensure that their pricing algorithms are programmed in a way that do not learn to signal future price increases in absolute percentage well before prices are available to consumers, and that they do not automatically match others' similar future pricing signals.

At the same time, businesses should arguably remain free to use self-learning pricing algorithms once prices are set and signaling can benefit consumers — for example, by allowing quicker and automatic switching, like smart meters detecting signals of lower or higher prices and self-learning to switch to the supplier offering lower prices. The debate is likely to continue and intensify throughout 2021 and beyond.

9. The Splinternet

A number of countries, such as Russia, China, Indonesia and Vietnam, have enacted data sovereignty legislation aimed at keeping the personal data of their nationals stored on servers within the country. Others, like Estonia, are considering a data embassy model, storing copies of their most important records overseas in order to protect them in case of outages, equipment failures or cyberattacks.

The General Data Protection Regulation and other data localization laws will impact the volume of international transit between operators. Law enforcement authorities, in particular, are concerned by the data being stored abroad, as the case of U.S. v Microsoft shows — with data of U.S. individuals being held on an Irish server, which is now being heard by the U.S. Supreme Court.

By contrast, the EU regulation on free flow of nonpersonal data should make it possible to keep nonpersonal data anywhere within the EU, as long as measures are in place to comply with data disclosure requests for law enforcement in individual member states.

Thus, a key issue for ensuring compliance with data localization laws for international operators will likely be having the appropriate data retention and disclosure protocols in place to respond to multiple requests for law enforcement.

10. Brexit

Last but not least, the regulatory concerns and complications from the exit of the U.K. from the EU will magnify as the transition period is now over. The U.K. has historically had a strong influence on EU telecommunications rules, particularly as an advocate for a less heavy-handed regulatory approach.

Without this voice but with the need to still access the single market, it remains to be seen if the U.K.'s Office of Communications will, too, have to become more interventionist. Other issues where the U.K. might then diverge includes roaming and certain net neutrality provisions. There have been a number of indications that post-Brexit the Competition and Markets Authority may become more officious based on political motivations.

The Competition and Markets Authority has developed a reputation for taking a tough line on mergers in recent years. More than a third of in-depth merger investigations opened in the U.K. in the last decade have resulted in outright prohibition or abandonment, with a significant share of the remainder requiring the businesses to offer remedies, such as promising to divest certain assets, to secure clearance.

The Competition and Markets Authority appears to have become even more interventionist of late, with eight of the 12 in-depth merger investigations it opened in the last three years leading to prohibition or abandonment; only two resulted in unconditional clearance.

This is a far lower success rate than businesses have achieved with the European Commission over the same period. However, only time will tell how the CMA's jurisdiction over a range of mergers that would previously have been the exclusive purview of the European Commission will play out in practice in relation to the communications industry.

Conclusion

2021 could be a watershed year for the digital markets industry. Some of these changes are so significant that they are likely to change the digital landscape, both in Europe and across the world, for years to come.

Francesco Liberatore is a partner and James Konidaris is a senior associate at Squire Patton Boggs LLP.

Matthew Kirk, an international affairs adviser at the firm, contributed to this article.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.