Doubling down, not backing down: defending the EU's digital sovereignty in the Trump era

by Max von Thun, Georg Riekeles and Pencho Kuzev

EPC EUROPEAN POLICY CENTRE
KONRAD ADENAUER STIFTUNG
OPEN MARKETS INSTITUTE

Introduction

The European Union (EU) is founded on the rule of law, with independent, democratically elected institutions that ensure the strongest protection of fundamental rights and values. Any company – European or not – that wishes to operate in the EU market must comply with the legal framework of the Union and its member states. However, over the past months, the EU, various member states, and democratic leaders have faced relentless attacks from U.S. tech billionaires with direct influence in the White House. Europe has been accused by U.S. tech platforms of censorship, stifling innovation through overregulation, and unfairly targeting them with enforcement actions inaccurately described as "tariffs". President Donald Trump, Vice-President JD Vance and other leading Republicans have themselves issued a series of threats, promising not to let Europe "take advantage of our companies" and even using NATO funding as a bargaining chip.

These accusations conveniently ignore that these same corporations have benefited massively from open access to the European market, the world's largest digital service market outside the U.S., while being responsible for inflicting huge damage on Europe's economy and democratic institutions. In 2021, the U.S. exported $283 billion in digitally-deliverable services to Europe, almost twice the amount going the other direction, and more than double U.S. exports to the entire Asia-Pacific region. At the same time, through their monopoly power and anti-competitive practices, U.S. gatekeepers have exploited the consumers and businesses dependent on them and stifled the emergence of European innovators. Most ominously, Europe's societal and democratic fabric is reeling from the multiple shocks of systemic amplification of mis- and disinformation, calculated distortions of European electoral processes, and the general degrading of Europe's public space through the promotion of conspiracies, hate speech or other illegal and extremist content.

Europe, along with other democratic nations such as Australia, Canada, Japan, and the UK, has made significant efforts to address these harms by investigating abuses, imposing remedies, and passing new legislation. Europe has also led the way internationally and across the Atlantic in attempts to establish common standards for tech governance. Over the years, efforts to rein in the tech giants have faced determined opposition from various U.S. governments who view these corporations as "national champions" and vectors of American power. Under the Biden administration however, a major shift took place, leading to broad alignment on the nature of the threats and the required response – particularly on the question of antitrust and market power.

With Trump's return to the White House, this brief window of opportunity has closed. Europe now faces a U.S. government resolutely opposed to any attempts to regulate its domestic tech giants, and willing to use aggressive measures to retaliate. While some might see this as an opportunity to dial down enforcement in the hopes of appeasing Trump, this would not only be a huge tactical blunder but also a dangerous surrender of Europe's fundamental values. Any sign of weakness will be ruthlessly exploited by the current U.S. government, which would only be more emboldened to issue further threats against European sovereignty. And it would extinguish any remaining chance Europe has of addressing its dangerous dependencies on tech monopolies and reversing the accelerating "algorithmification" of society, politics and democracy, further degrading our digital public square into a place where '*everything is possible, and nothing is true*'. **Instead of backing down, it is time for Europe to double down.**

Making full use of the EU's powers: A new enforcement paradigm

Over the past 15 years, the EU has taken an incremental approach towards addressing the ever-growing power of the tech giants. The European Commission has opted for modest measures in response to Big Tech's abuses, with tougher interventions only being contemplated as a last resort. This incrementalism is evident in the application of targeted measures for specific illegal behaviour against the same corporations over many years, and a reliance on narrow and weak remedies. This approach has failed to address the root of the problem – the tech giants' monopolisation of essential digital services and infrastructure, and their repeated abuses of this power.

As a result, the EU has been unable to meaningfully dent Big Tech's dominance, which has only grown. Instead, Big Tech has pursued strategies of **systematic interference and non-compliance**, supported by a growing army of lobbyists and lawyers. Fines – even those in the billions of euros – have been absorbed by these corporations as an acceptable cost of doing business, while misinformation, abuse and online surveillance have continued to proliferate and worsen, and are likely to accelerate further in today's political climate. Self-regulation, such as the EU's Code of Practice on Disinformation, has led to superficial initiatives that fail to address root causes while leaving underlying business models intact.

This is not to deny that important progress has been made in recent years. In response to the limitations of traditional antitrust, the Digital Markets Act (DMA) was introduced to promote fairness and contestability in the tech sector. This landmark legislation builds on lessons learned from previous antitrust investigations by imposing *ex-ante* rules on digital gatekeepers outlining strict 'dos and don'ts'. The Digital Services Act (DSA) gives the Commission significant new powers to hold tech giants accountable for unsafe and illegal content on their platforms. The AI Act will help ensure that artificial intelligence – particularly the powerful foundation models developed by large tech firms – is deployed legally, safely, and ethically in Europe. Finally, since all of these issues are also data problems, the General Data Protection Regulation (GDPR) remains potentially decisive, though it has yet to be seriously applied to the problem.

This growing regulatory arsenal will only achieve results if it is used with determination and imagination, with the toughest measures on the table from day one. The first months of implementing the DMA and DSA have demonstrated a willingness to enforce the law within a very short timeframe. Enforcement procedures were transparently initiated and developed based on objective criteria, and the Commission did not hesitate in investigating potential non-compliance by the platforms.

Yet with the change of administration in Washington, the context for enforcing these laws has shifted dramatically. Direct attacks on the integrity of Europe's public space, and on the EU's *right to legislate* in the most fundamental sense, have been met with a troubling silence from the von der Leyen Commission on its resolve to ensure continued and robust enforcement independent of political shifts in the U.S. The recently published Commission Work Programme 2025 – *Moving Forward Together: A Bolder, Simpler, Faster Union* –does not meaningfully address these concerns, and if anything, the signals sent out have suggested a readiness to back down on EU tech enforcement. Most worryingly, the absence of political leadership has created a dangerous void on how the EU intends to defend against existential threats, with only some member states such as France and Spain speaking up in defence of the EU's digital rulebook, while most others have remained silent.

Europe now faces a stark choice: to stand firm or to succumb to the orchestrated pressures from Big Tech and

their political allies. The latter would not only embolden the Trump administration and Big Tech, but also send a terrible signal to the European public, the wider tech sector, and international allies. Without rigorous enforcement to break open the tech giants' walled enclosures, entrepreneurs and innovators have little chance of launching and scaling their ideas. Europe's dangerous dependency on Big Tech platforms and technology would only increase, along with all of the implications that has for the continent's democracy, prosperity, security, and sovereignty.

Instead, the EU needs to double down on its digital rulebook and competition powers, ensuring that ongoing investigations continue at full pace while simultaneously considering bolder measures. As part of the EU's graduated repertoire of available actions, three specific tools which the European Commission should consider making use of are: **(a) restrictions on the ability to provide services; (b) antitrust action and corporate breakups; and (c) anti-coercion response and associated trade restrictions.**

(a) Restrictions on the provision of services in the EU should be considered where the behaviour of a tech giant seriously harms the Union's security, democracy, or other fundamental values of the EU. The potency of bans is demonstrated in Brazil, where X only complied with a Brazilian law on content moderation after its ability to provide services in the country was suspended. Like break-ups, such restrictions serve both as a deterrent – giving platforms a strong incentive to comply with the law – and as a powerful tool for eliminating serious harm or threats. The EU has several tools to block market access if necessary.

Under the DSA, the Commission holds direct supervision over "very large online platforms" as regards their content moderation, data practices, recommender systems, and algorithms, with wide powers to enforce EU rules across four categories of systemic risks: (i) the dissemination of illegal content; (ii) impact on the exercise of fundamental rights; (iii) effects on democratic and electoral processes, civic discourse, and public security; and (iv) effects on public health, minors, physical and mental well-being, or gender-based violence. As *ultima ratio* within the EU's graduated response, temporary suspensions are possible under Articles 51(3) and 82 of the DSA by seeking an order from the competent national judicial authority. In the case of urgency and risk of serious damage, the Commission additionally has the power to order interim measures based on a *prima facie* finding of an infringement (Article 70) or to take crisis response measures (Article 36).

In line with the EU Charter of Fundamental Rights, the safeguards against censorship (real or imagined) are strong. DSA bans are subject to highly restrictive conditions, including that the infringement cannot be addressed by "*other powers available under Union or national law*" and must entail "*a criminal offence involving a threat to the life or safety of persons*." All decisions taken by the Commission are subject to a right of defence and review by the Court of Justice of the European Union.

The GDPR also allows temporary or permanent bans on data processing, which could in effect amount to partial or complete bans on market access for platforms with data-intensive business models. This approach was used to block first ChatGPT (later reversed) and then the Chinese AI app DeepSeek from operating in the Italian market by the country's data protection authority. Most urgently, the GDPR's protections for "special category data" can protect European politics from manipulative algorithms.

In addition to making the full use of these existing provisions, the EU should consider expanding its powers to limit or cut off services of platforms that pose a serious and immediate threat to the EU's security, sovereignty or democratic institutions, as it did in response to Russian aggression and interference. For example, in addition to mandating more forceful and rapid action on recommender systems, bots, and other forms of manipulation, the DSA could be amended to allow permanent bans where a platform engages in election interference, espionage, or foreign propaganda.

The Commission's DSA enforcement thus far: due process or dangerously kicking the can down the road?

As the dominant major information platforms dismantle content moderation one by one and President Trump issues an Executive order on "overseas extortion and unfair fines and penalties", enforcement of the EU's digital rulebook has acquired new democratic and geopolitical urgency.

Yet the Commission's enforcement of the DSA is proceeding at a very different pace. In the case of Meta for example, enforcement remains at the stage of opening of proceedings and requests for information. In the case of the Twitter International Unlimited Company, also known as X, the Commission has reached the preliminary findings that the platform is in breach of the DSA as regards the use of dark patterns, advertising transparency, and data access, but has not yet moved to the stage of an enforcement decision. As regards the functioning of X's recommender systems, virality of accounts, and absence of content moderation, Commission enforcement remains at the stage of information requests and retention orders, perhaps tellingly, running until the end of 2025.

While EU platform bans understandably must clear a very high threshold, the weeding out of inauthentic use, automated behaviours, bots, and fake accounts that contribute to widespread dissemination of disinformation should be a matter of immediate action and compliance by platforms. Similarly, the EU should take a much stronger stance against recommender systems and their ability to amplify or suppress content with little transparency or accountability. Such systems are not necessary for an open digital public square but, conversely, can do great harms to it. None of these actions could be considered censorship, and indeed would help foster healthy public debate.

(b) Antitrust and breakups are critical tools in addressing the root causes of concentrated market power; even the mere threat of them can be an effective means of disincentivising harmful conduct. Structural remedies are allowed under the EU's competition laws, but in practice have been rarely used. This is beginning to change. The Commission is currently exploring breaking up Google's AdTech monopoly as part of an ongoing antitrust investigation, although it is taking far too long to reach a decision. Yet structural remedies could be used far more widely than this, as means of dispersing the concentrated power of tech monopolies, resolving the conflicts of interest that arise from their control of vertical supply chains and digital "ecosystems" and creating room for challengers to emerge. In fact, this is a rare issue on which the U.S. and the EU remain largely in alignment; the EU only formally began considering structural remedies after the U.S. Department of Justice proposed them, and – so far at least – the Trump administration has not signalled its intent to abandon ongoing efforts to break up Google, Meta and other tech monopolies, several of which were initiated during the first Trump administration.

Fully unlocking the potential of structural remedies may require minor adjustments to EU legislation, including removing the bias towards behavioural remedies in Regulation 1/2003 (which establishes the procedural framework for EU antitrust enforcement) as repeatedly called for by the European Parliament (EP), and amending the DMA to lower the bar for applying structural remedies, under which these are currently only available as a "last resort" subject to significant procedural hurdles.

(c) If the Trump government acts on its threats and tries to coerce the EU into not enforcing its democratic laws on Big Tech corporations, the EU must respond accordingly by means of its **anti-coercion instrument (ACI).** Adopted in 2023, this instrument has its origins in the lack of available tools for responding to Chinese trade measures targeting specific member states and U.S. secondary sanctions in 2018 under the first Trump presidency. The ACI is designed precisely to respond to situations in which a "*third country applies or threatens to apply a third-country measure affecting trade or investment in order to prevent or obtain the cessation,*

modification or adoption of a particular act by the Union or a member state, thereby interfering in the legitimate sovereign choices of the Union or a member state".

Where it is determined that economic coercion is taking place, the ACI allows the Commission to deploy a broad set of retaliatory measures in response listed in Annex I of the Instrument. This includes duties and restrictions on goods and services exported into the EU, exclusions from public procurement processes, restrictions on investments, and the revocation of protections on intellectual property.

Such trade restrictions can in principle be applied across the U.S. economy, but given the role of Big Tech in advocating and pressing for President Trump's aggressive trade and technology stance, it would not be unreasonable for retaliatory trade restrictions to target those same firms. It is not difficult to see how these measures could be used to inflict serious economic damage on Big Tech corporations, or to prevent them from operating in the EU market entirely. Under Annex I (f) there is a broad, general possibility to impose measures affecting trade in services, which, in principle, could be used to enforce service provision restrictions and platform bans in the EU. That said, more graduated and non-escalatory responses are more probable. For example, tariffs and import controls could be targeted to inflict maximum damage on specific firms closely associated with the administration, such as Tesla vehicles and Starlink equipment. Alternatively, dominant cloud providers could be banned from securing lucrative public sector contracts and from investing in data centres in the EU.

Crucially, the ACI gives the Commission formal powers to cooperate with other third countries in responding to economic coercion, an important provision given that the EU is unlikely to be the only government facing U.S. retaliation for its efforts to regulate the tech sector, as President Trump's Executive order of 21 February highlights.

Gearing up for success: six key actions

The EU's enforcement actions do not take place in a vacuum, but in a volatile and increasingly zero-sum geopolitical and geo-economic context. Success in reining in the tech giants requires not just bolder use of the EU's formal powers, but a strengthening of the vision, institutions and processes through which those powers are enforced.

1. **Understanding the true nature of the threat:** Enforcement of the EU's competition laws and digital rulebook has been hampered by a failure to fully grasp the threat posed by the dominant tech platforms. The harms caused by these corporations tend to be defined narrowly and in isolation from each other, whether the issue at hand is open and fair competition, harmful content, misinformation, harm to minors, AI safety, copyright or privacy. The result is a duplication of efforts and narrow, ineffective remedies. The Commission should replace this fragmented approach with a unified vision that treats all of these harms as resulting from the extreme scale and market power held by the tech giants. More fundamentally, the EU should move to recognise these corporations as essentially *political* actors that pose a direct threat to Europe's sovereignty, security, and democratic institutions. The broad portfolio of Commission Executive Vice-President Henna Virkkunen, uniting tech sovereignty, security, and democracy, provides the ideal opportunity to adopt this vision, which must be fully seized by the Commission's political leadership.

2. **Breaking down silos:** In parallel to adopting this unified vision, the Commission must break down the institutional barriers that stand in the way of effective coordination. There is currently far too limited interaction between different Directorates-General (DGs) and regulators responsible for regulating the conduct of tech platforms, including DG COMP, DG CONNECT, DG JUST, DG TRADE, the European Data Protection Board (EDPB), and the European Data Protection Supervisor (EDPS), although the joint COMP-CONNECT DMA enforcement team is an important and welcome exception. These silos prevent the Commission from drawing on relevant expertise spread across different departments to design holistic interventions that tackle Big Tech's conduct and market power in a joined-up way. For example, data protection regulators currently have little

involvement in digital merger and antitrust investigations, despite the clear role data dominance plays in entrenching Big Tech's economic dominance. A recent paper by the Konrad Adenauer Stiftung calls for the immediate establishment of a "Digital Enforcement and Resilience Taskforce" as a means of providing this much-needed coherence, which would bring together "Chief Enforcement Officers" from key DGs.

3. **Scaling up and unblocking resources:** As the EU has expanded its enforcement toolkit, lack of resources has become an increasingly urgent problem. The DMA, DSA, and the AI Act have all been hamstrung by recruitment and resource gaps, and underfunding has been a long-term constraint on the effectiveness of the EU's competition powers. This is a problem in itself, but even more so when the Commission is taking on some of the most powerful and well-resourced organisations in the world, able to deploy armies of lawyers, experts and lobbyists to delay or stifle enforcement. Given the increasingly existential threat posed by the tech giants to Europe's sovereignty and security, the EU should rapidly scale up the financial resources it allocates to supervising them. While this should be reflected in the EU's next long-term budget, this does not take effect until 2028, meaning interim funding is needed. This could be achieved in several ways, including imposing additional supervisory levies on dominant tech firms (building on the example of the DSA), reviving the idea of an EU-wide digital services tax that partly or wholly funds enforcement, or allocating a proportion of the fines collected by Big Tech back to regulators.

4. **Mobilising civil society and promoting transparency:** Civil society, including think tanks, consumer rights organisations, human rights advocates and digital rights activists, have played a central role in researching and highlighting the harms posed by Big Tech, developing practical policy solutions to address them, and mobilising policymakers to implement them. The EU institutions – the Commission and Council in particular – should be more proactive in engaging with civil society organisations (CSOs), which typically enjoy far less access to key decision-makers than industry. Doing so is a matter not only of providing the EU with valuable expertise, ideas and potential partners for its enforcement efforts, while ensuring that the voices of European citizens are heard, but more fundamentally about building and committing to a wider 'tech control'-agenda and ecosystem. Greater transparency in the Commission's enforcement processes, which – while increasingly participative – are still too opaque, would make it easier for civil society actors to identify opportunities to engage. In this context, a step in the right direction would be the establishment of formal structures for engaging with civil society organizations. Moreover, the EU and its member states should develop a mechanism to address the funding gap created by the recent actions of the Trump administration, which have highlighted the reliance of many European civil society organisations on U.S. government funding.

5. **Building political commitment:** Strong political commitment across the EU's institutions, member states, and political groups will be essential in providing the stable and resolute backing for robust enforcement against Big Tech. President von der Leyen's creation of a broad Executive Vice-President portfolio to address tech sovereignty, security, and democracy was an initial signal of determination, but the first months of this mandate have not been encouraging and political will seems since to have evaporated. This is therefore also the moment for other institutions to play their full role, not least the European Parliament. One way of enshrining this commitment would be to create a new special committee in the EP dedicated to monitoring and responding to the tech monopoly threat, modelled on the "Democracy Shield" special committee recently established to counter foreign interference, or a temporary inquiry committee as used in the case of the recent Pegasus investigation and in the context of CIA-led operations in EU countries in the early 2000s. Finally, where political will is lacking at the national level, the EU and other member states should bring all the necessary pressure to bear on Ireland, Luxembourg and other member states that are not meeting their responsibilities to fully enforce the GDPR and other EU legislation on the tech giants they host.

6. **Strengthening global alliances:** Given the aggressive stance of both the Trump administration and Big Tech, the EU must be ready to stand firm against retaliation in response to its enforcement measures. Standing firm will be easier if the EU is united alongside other governments that share its assessment of the threat and its resolve to address it, from Canada, Brazil, and India to the United Kingdom, Norway, Japan, New Zealand, and Australia. This global alliance against tech monopolies should include collaboration on both policy solutions – from competition and AI and data regulation to industrial policy and trade – and on joint responses to U.S. intimidation and retaliation.

Conclusion

Ceding the playing field to Big Tech in fear of retaliation from Trump will not lead to peaceful or productive relations between the EU and the U.S. On the contrary, as the new U.S. government seems determined to challenge Europe across several existential issues, including on the future of Ukraine and European security, such timidity will only result in further interference and bullying. It will also likely embolden these same corporations, further fuelling the polarisation that is causing irreversible damage to Europe's democracy and core values.

Reluctance to challenge and where necessary break up the algorithmic and monopoly powers that these tech giants enjoy, be this under the DSA, DMA or competition law, will jeopardise – perhaps permanently – the prospects of building a thriving European democracy and economy grounded in European values, with potentially irreversible consequences for Europe's prosperity and sovereignty as a whole.

The message must be clear: Europe's digital sovereignty is not for sale, at any price.