Berlin, November 2024
Analysis and Consulting

KONRAD ADENAUER STIFTUNG

MONITOR

INNOVATION/DATA POLICY

Creating the Space for Competitive and Resilient Digital Europe

Streamline Enforcement or Risk Prosperity and Safety

Dr Johnny Ryan FRHistS, Felix Kartte, Dr Pencho Kuzev

- Very large non-EU technology firms dominate our market by breaking our law.
- For Europe's SMEs and startups to scale up, it is not enough to invest in our infrastructure and innovation. We must clear space in the market for SMEs and startups to grow, so that they are not snuffed out by giant non-EU technology firms that refuse to respect European law.
- Enforcing EU law against giant non-EU firms is essential for the competitiveness agenda. It will also protect children, our elections, and Member States' security.
- We propose a Taskforce of Chief Enforcement Officers for a whole-of-Commission approach to coherently use diverse enforcement tools (under DSA, DMA, GDPR, NIS 2, etc.) for strategic objectives, without the need to further legislate.
- The GDPR has an important role to play in competitiveness. Full and proportionate enforcement against giant non-EU firms in Ireland and Luxembourg that misuse Europeans' data will create space in all Member States for Europe's SMEs and startups to scale up.

Table of Contents

Introduction

Giant non-EU technology firms dominate our market by breaking our law. Even with a strategic investment in innovation and capacity, Europe's innovators will not be able to scale unless space is created for them in the market. Robust enforcement of Europe's law against the giant firms that break our law can create that space. President von der Leyen has articulated a plan to revitalise Europe's competitiveness in the upcoming European Commission mandate. She has rightly eschewed major new legislative acts and focuses instead on cutting red tape to make business easier, and robust enforcement to curtail the power of these digital giants.

A handful of giant Chinese and U.S. tech firms dominate Europe's digital infrastructure, platforms, and media. This undermines the EU's ability to safeguard children, protect elections and national security, and support business growth.

We propose a way forward for the President. First, we summarise four critical digital challenges facing Europe, and the tools to solve them. Then, we propose a "whole-of-Commission" mechanism to coherently deploy those tools.

Four critical digital challenges, and the tools to solve them

Europe faces four major digital problems:

1. Competitiveness and digital sovereignty

The Letta Report highlights the economic and strategic imperative of scaling up Europe's companies to compete with Chinese and U.S. giants. Chinese and U.S. firms dominate digital

markets, suppressing European start-ups and SMEs.[1] Google and Meta control 50% of the global digital advertising market, while Amazon, Microsoft, and Google hold over 70% of Europe's cloud infrastructure market, creating a stranglehold on European AI startups. As the Draghi report notes, the largest European Cloud firm has just 2% of Europe's current market.[2] These firms also control the entire A.I. value chain, blocking European innovation.[3] Europe is critically dependent on Chinese and U.S. technology for consumer services, public services, and elements of critical infrastructure.[4]

President von der Leyen has announced investments to help EU SMEs and startups scale (including new supercomputing capacity for A.I. startups, and an "Apply AI Strategy" to boost industrial use of A.I). But no investment in infrastructure and innovation will scale Europe's SMEs and startups unless space has first been created for them in the market. We must assert European values against giant Chinese and U.S. firms that refuse to respect EU law. Enforcement against these undertakings is essential to the competitiveness agenda. Giant Chinese and U.S. firms have placed all their bets on Ireland (and Luxembourg, in Amazon's case) in the hope that they will operate as a data haven, where a failure to fully apply the GDPR will allow them to continue the misuse of personal data that aids their dominance of the EU market.

For Europe's SMEs and startups to scale up, it is not enough to invest in our infrastructure and innovation. We must clear space in the market for them to grow, so that they are not snuffed out by giant non-EU technology firms that refuse to respect the Single Market's rules and Europe's hard-won fundamental rights and freedoms. Fair and proportionate GDPR enforcement in Ireland would have a decisive impact on Chinese and U.S. firms across Europe, but would not impact European SMEs and startups. Enforcement of our values is an investment in our sovereignty and competitiveness.

President von der Leyen should ensure that Ireland and Luxembourg fully apply the GDPR against the giant firms that create the proportionately greatest risk to European's personal data. Although petty GDPR enforcement has terrorised SMEs and startups, there has been little substantive enforcement to curtail giant Chinese and U.S. firms' data misuse.[5] These giants are highly vulnerable to GDPR enforcement because they misuse personal data at such massive scale, and rely on internal data free-for-alls to dominate the market. This will not increase the regulatory burden on SMEs and startups across Europe. Indeed, it may reduce it, by cutting back the sham "compliance theatre" giant tech forms have imposed on the market.

Fair and proportionate enforcement will create space in the entire EU market for SMEs and startups to scale up. A modest investment of political capital is required. The Commission should be prepared to launch infringement procedures. In parallel, vigorous enforcement of the Digital Markets Act (DMA) can contribute to interoperability and may reduce market concentration in the A.I. value chain and cloud infrastructure.

2. Harm to children

President von der Leyen has announced an EU-wide inquiry into the impact of social media on the well-being of young people. Some observers warn of a youth mental health crisis.[6] TikTok executives' leaked chats reveal their knowledge that the platform's algorithm harms children. [7] TikTok pushes pro-suicide videos at vulnerable children.[8] YouTube promotes extreme hatred of women in young boy's feeds.[9] The common factor is the toxic algorithms that use intimate data

about children to push a personalised stream of despair and self-loathing into their social and video feeds.

Commission enforcement of the Digital Services Act (DSA), combined with a more robust Member State enforcement of the Audio-Visual Media Services Directive (AVMSD), may curb algorithmic promotion of content harmful to kids, and enforce against addictive design. Most decisive may be enforcement of GDPR protections for "special category data", which would force these platforms to switch off toxic algorithms by default.

3. Foreign interference

President von der Leyen announced the "Democracy Shield" to fight foreign interference. Europe is saturated by foreign surveillance. Tens of thousands of Chinese Hikvision and Dahua CCTV cameras are installed in Member States[10] – including in political facilities.[11] In parallel, the dangerously insecure technology at the heart of the U.S.-built online advertising system sends compromising data about sensitive EU personnel to China and Russia.[12] The same online advertising system exposes our citizens to illicit profiling by a murky industry of data broker firms, who peddle their secrets to the highest bidder.[13] European security and safety is further threatened by Russian propaganda and election interference within the EU and in candidate countries, which is facilitated by "big tech" firms.[14]

Foreign digital surveillance should be stopped by enforcement of the GDPR and NIS 2. In parallel, integrating "Democracy Shield" threat analysis into the DSA framework would enhance effectiveness without duplicating efforts. Finally, concerted enforcement against giant non-EU firms may give the Commission leverage to stop adversarial interference in elections on our borders.

4. Threats to democracy

The quality of information in our society is declining. There are at least two causes. First, disinformation and hate is being artificially amplified by the same toxic algorithms that harm our children on non-EU digital platforms.[15] Second, the journalism business is being destroyed by the broken and fraud-riddled online advertising market, whose rules are defined by "big tech" firms. The data free-for-all in online advertising allows untrustworthy websites to trade off trust-worthy journalism's commercially valuable audience data,[16] and facilitates an estimated €78 billion annual fraud[17]. This data free-for-all also allows foreign entities to build intimate profiles of EU voters, and micro-target them with deceptive ads.

The disinformation problem will be remedied by the same measures proposed above to protect children from toxic algorithms. The collapse of journalism at the hands of the broken online advertising system will be remedied by GDPR enforcement to stop the data free-for-all. Enforcement would favour trustworthy journalism and protect voters against dangerous profiling.

If robustly enforced, the DSA may also help by limiting discrimination against publishers by search engines and platforms, improving the transparency of tracking-based advertising, and prompting better respect for Member State's electoral and media rules. The DMA may also help by forcing fair treatment of media products in app stores.

Europe has a range of useful enforcement tools at its disposal to confront these critical problems (table on next page). What the Commission now requires is a mechanism to marshal and coherently deploy them.

Table: Key enforcement tools, mapped to the President's Political Guidelines

OBJECTIVE	TARGETS AND PROBLEMS	EXISTING TOOLS	TASKFORCE ACTIONS	VENUE
Political Guideline: A new plan for Europe's sustainable prosperity and competitiveness				
Create space for Europe's start-ups and SMEs and A.I.	**Google, Microsoft, Apple, Meta, TikTok, Amazon, Shein, Temu** Cascading monopolies based on internal data free-for-alls	A. GDPR Article 5(1)b , and Article 6 B. DMA Article 5(2), Article 6(2) and (9) and (10), Article 12 and Article 14(1) C. DG Competition merger assessment rules (amending to include forensic analysis of companies GDPR Article 30 records of processing activities)	A. Political pressure on Ireland (threaten infringement procedure if necessary) and Luxembourg (Amazon). B. Rapid action within DG Competition and DG Connect. C. Rapid action within DG Competition.	A. Data protection authorities in Ireland and Luxembourg. B. DG Competition C. DG Competition
Political Guideline: Supporting people, strengthening our societies and our social model				
Protect children and teens from toxic algorithms that promote self harm and suicide	**Tik Tok, YouTube, X, Instagram, Snapchat, Facebook** Intimate profiling exposes vulnerable children to a personalised diet that promotes self loathing, and glamourises self harm and suicide	A. GDPR Article 9 B. AVMSD Article 6a(1), Article 28(1)	A. Political pressure on Ireland (threaten infringement procedure if necessary) B. Support for use of AVMSD by national authorities	A. Irish data protection authority B. National audiovisual media services supervisory authorities
Political Guideline: A new era for European Defence and Security				
Protect national security (online profiling of sensitive personnel)	**Google, Microsoft, others** Large-scale data leakage exposes sensitive military, political, and industrial leaders and personnel to manipulation, blackmail, hacking, and undermining of their institutions	A. GDPR Article 5(1)f, 24, 25, 32, 35, 36 B. NIS 2, Article 32(4)	Political pressure on Ireland (threaten infringement procedure if necessary)	A. Irish data protection authority, and Dutch data protection authority B. National cyber security authorities
Protect national security (real world surveillance)	**Hikvision** the Chinese internet connected CCTV camera network (AS AN EXAMPLE) Large-scale surveillance conducted by foreign powers	A. GDPR Article 5(1)f, 24, 25, 32, 35, 36 B. NIS 2, Article 32(4) C. Proposed Regulation for the screening of foreign investments (2019/452), Article 13	A. Political pressure on the Netherlands (threaten infringement procedure if necessary) C. Finalise the Regulation and enforce Article 13	A. Dutch data protection authority B. National cyber security authorities C. Co-legislators
Political Guideline: Protecting our democracy, upholding our values				
Curb online disinformation, hate, and hysteria (including foreign interference and disinformation)	**Tik Tok, YouTube, X, Instagram, Snapchat, Facebook** Intimate profiling exposes susceptible people to a personalised diet of hate and disinformation	A. GDPR Article 6, Article 9 B. AVMSD Article 28(1) and perhaps in the absence of functioning and reliable age verification Article 6a(1) of AVMSD is applicable, too	A. Political pressure on Ireland (threaten infringement procedure if necessary) B. Support for use of AVMSD by national authorities	A. Irish data protection authority B. National audiovisual media services supervisory authorities
Protect elections and improve media sustainability (including foreign interference and disinformation)	**Google, Microsoft, other "RTB" online advertising exchanges** Large-scale data leakage in online advertising exposes voters to personalised disinformation and manipulation, and undermines media sustainability.	GDPR Article 5(1)f, 24, 25, 32, 35, 36	Political pressure on Ireland (threaten infringement procedure if necessary).	Irish data protection authority, and Dutch data protection authority

Source: Authors' own illustration

A Whole-of-Commission Solution

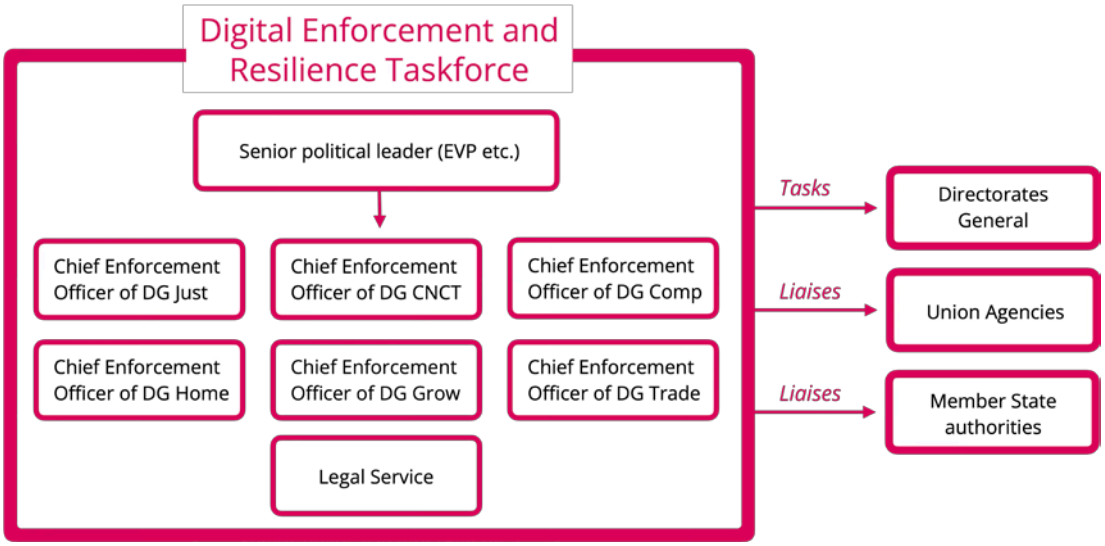
Europe has developed a powerful regulatory toolbox in the last two mandates to address these digital challenges. This will be complemented by the new measures President von der Leyen announced in her political guidelines. To reduce market fragmentation and coherently deploy Europe's tools, the Commission requires a new mechanism that unifies enforcement of its diverse regulatory powers against undertakings, including streamlined liaison with Member State authorities and coordination of powers. This mechanism can be rapidly introduced without legislation.

Digital Enforcement & Resilience Taskforce

The Commission should rapidly establish a Taskforce composed of Chief Enforcement Officers of Directorates General Connect, Grow, Just, Comp, Home, and Trade. These new roles should be senior, at Deputy Director General level, and focused on coordination. The legal service should also be present in the Taskforce, to advise on what is possible.

Taskforce should not deprive any DG of currently held powers and competences. Rather, it should enable early interservice consultation and the coordinated pursuit of objectives set by the political leadership.

Diagram: Enforcement Taskforce for a whole-of-acquis approach



Source: Authors' own illustration

Political leadership and support

The Taskforce should pursue objectives defined from time to time by a senior political chairperson, perhaps an EVP. This Chairperson would be similar to the Enrico Letta's proposal for an overall Chief Enforcement Officer.

Taskforce objectives should be endorsed by the College of Commissioners. This will enable each DG to accommodate themselves to the objectives, including where objectives fall outside a particular DG's particular area. Political leadership of the Taskforce would also enable the application of pressure on key Member States (for example, Ireland and Luxembourg).

If political leadership of the Taskforce is not desirable, then chairpersonship of the Taskforce should rotate between the Chief Enforcement Officers of the DGs, and held for a single year.

Chief Enforcement Officers
Each DG's Chief Enforcement Officer should coordinate enforcement within their respective DG. At the Taskforce they should work with their fellow Chief Enforcement Officers to pursue objectives set by the political leadership. They should also liaise with relevant Member State authorities to pursue those objectives, and have the necessary political support to do so.

The Taskforce is not intended to directly manage joint cases. Therefore, it may not be necessary to agree confidentiality arrangements.

Benefits
Unifying enforcement would also reduce Single Market fragmentation. But the Taskforce would also give the Commission a powerful toolkit to achieve its strategic objectives. The Commission would be able to deploy multiple legal instruments coherently against a single undertaking. At minimum, it would help DGs avoid pursuing the same sanction against the same target, which does occur. It would also increase the Commission's power versus giant undertakings. Their opportunities for malicious compliance would be reduced, and the odds of rapidly settling cases would rise.

Longer term development

In the longer term, the Commission may consider establishing an entity (Directorate General, Agency, etc.) that further coheres and unifies enforcement. This could enhance coordination and reduce bureaucratic overlap, and allow for interdisciplinary staff that are free of constraints of existing structures. It would also be an opportunity to establish procedural rules that insulate the body from political interference in technical enforcement.

1 https://www.ft.com/content/07bf9005-3aa1-47c1-a8b0-f8bf6f1975d7

2 https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf#page=22

3 https://www.openmarketsinstitute.org/publications/report-ai-in-the-public-interest-confronting-the-monopoly-threat

4 https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

5 https://www.economist.com/by-invitation/2023/05/24/dont-be-fooled-by-metas-fine-for-data-breaches-says-johnny-ryan

6 https://www.newstatesman.com/technology/2023/03/jonathan-haidt-social-media-dangerous-teenage-girls-anxiety-depression

7 https://www.npr.org/2024/10/11/g-s1-27676/tiktok-redacted-documents-in-teen-safety-lawsuit-revealed

8 https://www.rte.ie/news/primetime/2024/0416/1443731-13-on-tiktok-self-harm-and-suicide-content-shown-shocks-experts

9 https://www.isdglobal.org/isd-publications/algorithms-as-a-weapon-against-women-how-youtube-lures-boys-and-young-men-into-the-manosphere

10 https://www.shodan.io/search/facet?query=hikvision&facet=country

11 https://www.irishtimes.com/politics/2023/02/12/opposition-backs-call-to-remove-chinese-cameras-from-leinster-house

12 https://www.iccl.ie/2023/new-iccl-reports-reveal-serious-security-threat-to-the-eu-and-us

13 https://netzpolitik.org/2024/databroker-files-datarade-geschickte-geschaefte-im-graubereich

14 https://www.politico.eu/article/russia-plot-meddle-moldova-election-uncovered-say-western-allies-maia-sandu-kremlin

15 https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499

16 https://www.adweek.com/programmatic/advertisers-help-publishers-protect-data-bpa

17 https://searchengineland.com/ad-spend-lost-ad-fraud-2023-432610

Imprint

The Authors

Dr Johnny Ryan FRHistS is the Director of Enforce, and an Enforce Senior Fellow. He is also a Senior Fellow at the Open Markets Institute. Previously, Dr Ryan held senior roles in the online advertising, media, and technology industries.

Felix Kartte is a policy entrepreneur, technology expert and writer. He has extensive experience in developing strategies to regulate tech companies and counter digital threats, including disinformation. He started his career as a researcher and journalist and has covered digital democracy for outlets such as Süddeutsche Zeitung and Politico.

Dr Pencho Kuzev is a Policy Advisor for data and competition policy at the Konrad-Adenauer-Foundation, with a particular focus on the regulatory framework in Europe. He plays an active role in the T20/20 process and publishes on various topics related to the digital economy, such as the Digital Markets Act, European Cloud Policy, and Open Data. He is also the organizer of the European Data Summit.

Konrad-Adenauer-Stiftung e. V.

Dr Pencho Kuzev
Data & Competition Policy
Department Economy and Innovation
Division Analysys and Consulting

Pencho.Kuzev@kas.de

Published by: Konrad-Adenauer-Stiftung e. V.
Design and typesetting: yellow too Pasiek & Horntrich GbR

This publication was published with financial support of the Federal Republic of Germany.