European Parliament

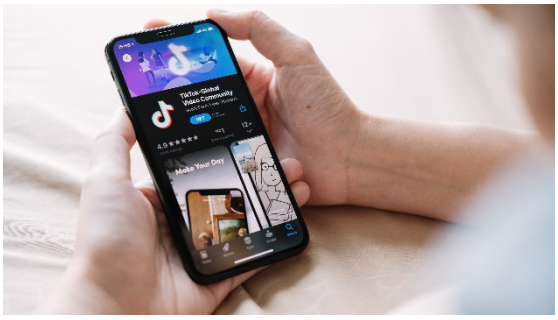
TikTok and EU regulation: Legal challenges and cross-jurisdictional insights

SUMMARY

While Europeans are adopting TikTok at a remarkable pace, recent headlines on addictive design, data protection violations, election interference, incendiary content and child sexual exploitation incidents are casting a shadow over its success. This briefing maps the key issues associated with the platform and outlines the European Union's (EU) legal framework to facilitate parliamentary discussions on recent developments, inform debates on future legislation such as the digital fairness act, and support the European Parliament's scrutiny of regulatory enforcement.

EU investigations into TikTok are ongoing, yet few final decisions are available, and reliable information is sparse. A review of incidents and initiatives in the United States and the United Kingdom provides relevant insights on topical issues relating to TikTok. For instance, hearings and lawsuits linked to the US divest-or-ban law reveal possible national security risks arising from TikTok granting Chinese affiliates access to user data. Lawsuits from at least 16 US attorneys general demonstrate TikTok's potentially addictive features. Parliament will review the results and formulate its position once EU enforcement actions and regulatory preparations conclude.

More than 10 EU laws regulate social media operations and services. For instance, rules in the Unfair Commercial Practices Directive, the General Data Protection Regulation and, as applicable, the Artificial Intelligence Act on fairness and non-manipulation can be invoked to mitigate risks like addictive design. However, precise legal applications remain unclear without established case law. This creates broad enforcement possibilities, but it also suggests a need for clearer guidelines or additional regulation. While enforcement actions may escalate geopolitical tensions with China, these issues could be eased through collaboration on shared priorities such as child protection, enhancing strategic and operational interdependence, and exploring privacy-enhancing middleware solutions.



IN THIS BRIEFING

EPRS | European Parliamentary Research Service

Author: Hendrik Mildebrath with Bente Daale
Members' Research Service

PE 775.837 – June 2025

Introduction

The current version of the online platform TikTok was launched in the EU in August 2018 after merging with 'musical.ly'. It allows users to create, share, and interact with short videos, offering a highly engaging experience. TikTok has revolutionised the consumption of short-form videos and inspired other social media providers to adopt similar features. As a hallmark of today's remix and reaction culture, TikTok attracts users seeking funny and creative content. Some attribute TikTok's success to the algorithm that selects content for the main feed, while others point to its innovative design as the primary driver of user engagement. Ultimately, both aspects work in tandem.

According to TikTok's recent Digital Services Act (DSA) transparency report, the platform has **159 million monthly** active users in the EU, representing roughly 35.5 % of the EU population. On average, active users globally spent almost **70 minutes per day** in November 2024 using TikTok's Android app, compared with YouTube, Facebook and Instagram, which stood at about 54.5, 34.5, and 32.5 minutes per day, respectively. The overwhelming majority of TikTok users are also active on other social media platforms, contributing to the total time spent on social media. The market research company GWI estimates that in 2023, users aged 16-64 spent an average of 2.26 hours per day on social media – with Gen Z averaging 2.51 hours. The trend discovery company Exploding Topics estimated that in June 2024, **25 % of TikTok users were between 10 and 19 years old**. Not all countries are covered by these statistics and usage behaviour varies based on region and age.

According to its 2023 financial statement, **TikTok Information Technologies UK Ltd. generated a turnover of €4.57 billion**. The company is the TikTok operator for users in the European Economic Area (EEA), the United Kingdom (UK) and Switzerland, and primarily generates revenue by distributing online advertising and providing other services, such as livestreaming, on the platform.

By comparison, according to their 2023 financial statements, Meta Platforms Ireland Ltd. generated approximately €69.75 billion in turnover with Facebook, Instagram, Messenger and third-party mobile applications. Google Ireland Limited generated €77.3 billion in turnover through Google websites and apps, including YouTube, and on properties of Google Network Members. In comparison to 2022, TikTok's revenue grew by 74.6 %, while Meta's and Google's grew by 20.1 % and 6.4 % respectively. While the comparability of these figures is limited,[1] they suggest that advertising on social media has proven to be particularly cost-effective for marketers. In March 2025, TikTok expanded its European social e-commerce operations from Spain and Ireland to France, Germany and Italy. Additionally, it may gain shares in the search advertising market as it increasingly becomes the search engine for Gen Z.

According to a study commissioned by TikTok, the platform contributed €4.8 billion to the GDP of five EU countries in 2023 (Belgium, Germany, France, Italy and the Netherlands). While research on the overall net welfare impact of social media is still in its early stages, studies show that many users would be willing to deactivate their social media accounts only for a substantial amount of money. While this initially seems to indicate a positive welfare impact, economists highlight that addiction, learning and projection bias may lead to suboptimal consumption choices (see Section on 'Public health' below). An experiment with university students found that many users highly value TikTok and Instagram– requiring an average of US$50 to stop using them individually – but are paradoxically willing to pay only US$24 and US$6, respectively, for their global deactivation. Sixty percent of TikTok users and 46 % of Instagram users experience negative welfare from the products' existence. The study suggests that many respondents would prefer a world without TikTok and Instagram but feel compelled to use them, for example, due to risk of social exclusion or fear of missing out.

Key issues

As varied as the forms of expression, content, functionality and misuse may be, so too are the potential risks they can pose. Many issues raised in relation to TikTok reflect broader industry challenges.

Data protection and privacy

In a 2024 special Eurobarometer survey on the Digital Decade, respondents cited personal data misuse (46 %) as their most impactful concern relating to digital technologies.

Like competitors, TikTok collects a wide range of data. This includes device information (IP address, keystroke patterns, activity across devices, search history, etc.) and approximate location data (triangulating SIM card or IP address data). Additionally, TikTok collects characteristics and features about the video, image and audio recordings (for example, the existence or location of a face or other body parts in an image), metadata (such as when, where and by whom the user content was created), and usage information (for instance, how the user interacts with ads or engages with other users, and the search history the user generates). The platform also grants foreign entities within its corporate group limited remote access to the data provided, as well as to automatically collected information and data from other sources to the extent necessary to provide certain functions such as storage, content delivery, security, research and development, analytics and content moderation. Additionally, data is shared with third parties such as advertisers, sellers and other service providers.

Reports released by cybersecurity firms Penetrum and Internet 2.0 draw attention to TikTok's excessive data harvesting and links to Chinese IP addresses. However, a 2021 analysis by the research lab CitizenLab concluded that the collection of data is 'not exceptional when compared to industry norms' and that TikTok does 'not appear to exhibit overtly malicious behaviour'. In 2023, the Swiss National Test Institute for Cybersecurity found no indications that users were being monitored, but stated that extensive permissions and vulnerabilities make it technically possible. It flagged that location data is frequently transmitted and that the communication is not end-to-end encrypted. Additionally, TikTok's backend server, whose contents are unknown, is encrypted.

Recently, TikTok has become the subject of various investigations and lawsuits relating to data protection and privacy violations. In Europe, the NGOs NOYB, SOMI and Ius Omnibus have filed complaints with courts and supervisory authorities, challenging TikTok's transfer of data to China, personalisation of the feed based on sensitive data, intrusive tracking on and off the platform, and opaque wording of its privacy policy and terms of service. The United Kingdom's (UK) Information Commission has announced investigations into how TikTok uses children's personal information and makes recommendations to them. In a similar vein, the US Department of Justice (DoJ) has sued TikTok for violating a 2019 FTC order and for failing to comply with the Children's Online Privacy Protection Act (COPPA) requirement to notify and obtain parental consent before collecting and using personal information from children under the age of 13.

A **central worldwide concern is whether TikTok transfers data to China, potentially compromising user data protection and privacy**. Despite TikTok's repeated claims to lawmakers and users that it does not, leaks from Project Texas – an initiative aiming to localise data and provide assurance – has revealed that Chinese-based staff accessed US user data with the aim of halting data access. TikTok then came under public scrutiny for surveilling US journalists who reported critically on the company, including the journalist who broke the story about Chinese access to US user data. TikTok CEO Shou Chew has promised more transparency and access to third-party independent monitors to ensure accountability and uphold TikTok's commitments. Additionally, TikTok has acknowledged that employees of ByteDance, the company that owns the platform, misused their access to track the journalists' location, but denies that it was for spying. In December 2023, the FBI and the US Department of Justice launched investigations.

A year after beginning the process of deleting protected US data from global data centres, TikTok was still working on this task in March 2024. Judicial proceedings revealed that TikTok's source code is developed and maintained by employees of a ByteDance subsidiary located in both the US and China. Additionally, the US government stated that it does not possess sufficient oversight or resources to effectively monitor the risk mitigation measures that TikTok pledged to implement. It also expressed a lack of trust in ByteDance's commitment to act in good faith to comply with these promises. US officials also cited data collection and transfers to China through an internal web suite

called Lark (also known as 'Feishu')[2] as evidence that Project Texas was failing to adequately address national security concerns. In response, TikTok's spokesperson stated that 'the government has never put forth proof of its claims'.[3]

On 2 May 2025, the Irish data protection authority (DPC) found that remote access to data of EEA users had violated the General Data Protection Regulation (GDPR) data transfer rules. Consequently, the DPC fined TikTok €530 million and ordered the suspension of data transfers despite ongoing changes brought about by Project Clover, an initiative similar to Project Texas but concerning EU data. At the time of writing, the DPC's decision was not public.[4] Previously, a range of data protection authorities (DPAs), including the Irish, Dutch and French ones had taken enforcement actions against TikTok for a number of data protection violations. By the end of 2023, TikTok had earmarked about €1 billion for possible administrative fines and compliance measures. In comparison, Meta Platforms IE Ltd. and Google IE Ltd. had earmarked around €4.16 billion and €1.5 billion, respectively. TikTok also launched privacy innovation efforts in 2023 and now provides privacy enhancing technologies and enhanced data security.

National security

In response to data access by Chinese affiliates, public authorities around the world, including the European Parliament, the European Commission and the Council of the EU, banned TikTok from corporate devices in 2023. In the US, policymakers under both the Biden and Trump administrations have taken extensive action to reduce the risks of Chinese access to sensitive data and to curb Chinese control over software and connected technologies. Under the Biden administration, Congress enacted the Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACA) in April 2024. This act prohibits the use of applications provided by TikTok's parent company ByteDance and empowers the president to extend the ban to other companies of a particular nature that pose serious national security risks. The prohibition becomes applicable within 270 days after the statutory enactment of the act or the presidential determination, unless the relevant companies execute a qualified divestiture or the president grants a one-time extension of not more than 90 days. The ban became effective with respect to TikTok on 19 January 2025, but US President Donald Trump delayed enforcement three times to enable the conclusion of a divestiture deal. The most recent delay postponed enforcement to 17 September 2025.

TikTok challenged the constitutionality of this act, but both the D.C. Court of Appeals and the US Supreme Court upheld it. They gave significant weight to the government's 'informed judgement'. The US government provided evidence that the People's Republic of China (PRC) poses a national security threat in general[5] and through companies like TikTok in particular. The two national security risks identified in these judgments were those of 'data security' and 'content manipulation'.

According to the D.C. Court of Appeals, 'The PRC poses a particularly significant hybrid commercial threat because it has adopted laws that enable it to access and use data held by Chinese companies'. Through control over Chinese parent companies, the PRC can also 'access information from and about U.S. subsidiaries and compel their cooperation with PRC directives'. As a result, the PRC can 'conduct espionage, technology transfer, data collection, and other disruptive activities under the disguise of an otherwise legitimate commercial activity'. Due to the vast amount of data collected by TikTok and its links to China, two consecutive US presidents have recognised TikTok as a major security vulnerability. As mentioned above in relation to Project Texas, the D.C. Court of Appeals also underlines that the government does not trust TikTok's proposed mitigation measures.

The PRC also uses its cyber capabilities to support its influence campaigns around the world. These global 'influence operations' aim to 'undermine democracy' and 'extend the PRC's influence abroad'. The US government reports that 'ByteDance and TikTok Global have taken action in response to PRC demands to censor content *outside* of China'. Regarding TikTok in the US, the government predicts that ByteDance and TikTok entities 'would try to comply if the PRC asked for specific actions to be taken to manipulate content for censorship, propaganda, or other malign purposes on TikTok US'.

Additionally, there is a powerful Chinese Communist Party committee incorporated into ByteDance through which the Chinese government can influence the company.[6]

Conversely, Professor Steven Weber argued on behalf of TikTok that these issues are not unique or even distinctive to TikTok. China-based subsidiaries of US technology companies are subject to the same disclosure rules (e.g. Cisco, Dell, and IBM), and some of them have established internal committees comprising members of the Communist Party of China. Many US companies, including Electronic Arts, rely on Chinese-based engineering teams to develop games and software products with millions of international users. Additionally, TikTok's response to data misuse by employees – including the firing of the personnel involved and the reinforcement of internal controls – matches industry standards. According to Steven Weber, there is no evidence of foreign interference in public perspectives and opinions using TikTok's algorithm. He cites academic findings that TikTok does not employ *overt* political censorship, as politically sensitive search terms ('Communist Party taboos') continue to return results. He also argues that concerns about pro-Palestinian content following the 7 October 2023 attacks are based on misinterpreted data. TikTok took a broad range of actions (p. 93 et seq.) in response to this crisis.

If TikTok shares user data with unaffiliated companies whose data is accessible to foreign governments – for instance, through deeper integration with the open display market or by sharing data with data brokers – this would heighten national security concerns further. The Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFA) prohibits data brokers from making personally identifiable sensitive data of a US citizen available to any foreign adversary country or entity controlled by a foreign adversary. The Electronic Privacy Information Center (EPIC) and the Irish Council for Civil Liberties (ICCL) filed the first complaint under the new PADFA Act, targeting Google's real-time bidding system. In the EU, the Court of Justice of the European Union (CJEU) has ruled that the consent management standard used in the open display market breaches the GDPR, and academics doubt that this standard could ever serve as a legal basis for real-time bidding.

Election interference

Another topical risk closely tied to national security is election interference. On 4 December 2024, Romania's outgoing President Klaus Iohannis declassified intelligence revealing that nearly 800 TikTok accounts – originally created in 2016 by Russia – had been reactivated in November to support presidential candidate Călin Georgescu. Additionally, 25 000 accounts had been activated two weeks before the first round of presidential elections. On 6 December 2024, two days before the elections' second round, Romania's Constitutional Court annulled them. In response, the European Commission initiated formal proceedings against TikTok in December 2024. Prior to the repeat elections in May, TikTok announced that it would set up a Romanian election centre to enhance the integrity of its platform.

The editor-in-chief of the TV network RT (formerly Russia Today), Margarita Simonyan, declared that RT is capable of 'conducting [an] information war against the whole Western world', and to 'conquer' and 'grow' audiences in order to access them in 'critical moments'. According to the US Intelligence Community (a group of US federal government intelligence agencies and subordinate organisations) and the Senate Select Committee on Intelligence, the US also experienced Russian election interference through social media during its 2016 presidential elections.

Public safety from criminal offences

A common public safety concern is the **spread of child sexual abuse material** (CSAM) through social media. While it appears likely malicious entities would use end-to-end encrypted communication services to exchange CSAM and avoid detection by law enforcement, they are also misusing social media platforms with standard encryption, such as TikTok. Reports have revealed that users are sharing passwords to private accounts in order to exchange CSAM and solicit others to contribute explicit material. Furthermore, TikTok's livestream feature (TikTok LIVE) has been misused to lure minors into performing sexual acts, rewarding them with virtual gifts that can be exchanged for

money (known as 'giftbaiting'). Once malicious entities obtain explicit material, they can engage in sextortion crimes. According to Thorn's 2023 report on online safety, TikTok ranked 5th among the top platforms where the highest percentage of minors reported having had an online sexual experience (11 %), with 6 % believing they had interacted with an adult. Similar conclusions can be drawn from a tipline report and a self-report survey of anonymous individuals searching for CSAM.

In June 2024, the Utah Attorney General and other US attorneys general (see the Section on 'Public health' below) filed lawsuits alleging that TikTok had consciously allowed young people to be sexually exploited on its platform in exchange for money, and that it had used manipulative dark patterns to keep them on LIVE. While TikTok provides minors of different age ranges with different features and default-settings, the attorneys general consider that the age gate is largely ineffective. TikTok scans user content, provides for human oversight, and on various occasions has cooperated with external partners and engaged with authorities. To help identify CSAM, TikTok uses multiple technologies, including own systems and hash-matching software like Microsoft's PhotoDNA, Google's Content Safety API, and YouTube's CSAI Match. In January 2024, TikTok was working on a model to detect grooming and predator behaviours within particular features such as LIVE.

Another public security risk linked to social media includes the spread of false information **and incendiary speech intended to stir up violence**. In the summer of 2024, rioters targeted mosques and hotels in the UK, driven in part by false claims spread on social media platforms regarding the killing of three children in Southport. Following the incidents, Ofcom reported that illegal content and disinformation spread rapidly online, driven in part by algorithmic recommendations that amplified divisive and harmful narratives. Despite reported efforts to curb such material, its proliferation appears to have contributed to the ensuing violent disorder, with several individuals subsequently convicted for online offences including incitement to racial hatred, threats of serious harm, and the dissemination of false information intended to cause harm. The Institute for Strategic Dialogue drew similar conclusions. Research indicates that social media can act as a propagation mechanism for violent crimes by enabling the spread of extreme viewpoints.[7] In a hearing before the UK House of Commons' Science, Innovation and Technology Committee, TikTok explained that it had identified the riots as a high-risk event and launched a command centre to curb the spread of videos and comments violating its community guidelines. TikTok involved 'more than 100 people across 10 teams, working on a 24/7 follow-the-sun basis that [they] were moderating around the clock'. TikTok reported that during the two peak weeks of the riots, its trust and safety teams removed tens of thousands of videos and comments. Difficulties lay in establishing authoritative sources of truth, particularly in the wake of fast-paced developments.

Public health

Growing concerns about the impact of mobile phones on children's well-being have prompted EU Member States to ban phones in schools and consider stronger parental controls and age verification measures. Against this backdrop, TikTok's highly engaging features are now under global scrutiny from regulators, lawmakers, and academics. While research shows that the health effects of social media on children vary depending on the context, small to moderate associations with adverse effects have been established (see Annex below for more details). Many experts and US attorneys general argue that TikTok's features pose specific health risks.

Since March 2022, TikTok has been under a 47-state investigation from US attorneys general regarding its practice of inducing children to use its social media platform, resulting in harm to them. As investigations continue and attorneys general seek to compel TikTok to preserve and produce relevant evidence, 14 attorneys general[8] launched independent legal action against the platform on 8 October 2024 citing its adverse effects on children. Their complaints underscore concerns about TikTok's **impact on adolescents' mental and physical health**, suggesting that the company was aware of these harms but failed to take appropriate action.

In particular, the complaints identify features such as the personalised For You Feed, beauty filters, autoplay, infinite scroll, TikTok stories, TikTok LIVE, push notifications, and likes and comments as

problematic. According to unredacted complaints from Kentucky and Utah, as well as related reports, internal studies and communications reveal that TikTok was aware of the harms it caused to children and failed to act. An internal study argues that TikTok's business model 'encourages optimization for time spent in the app'. The app is 'particularly popular with younger users, who are particularly sensitive to reinforcement in the form of social reward and have minimal ability to self-regulate effectively'. In the same vein, a report had flagged that users 'believed they spent too much time in the app'. Attempts to resolve user concerns over excessive use through a default time prompt at 60 minutes had a negligible impact, but TikTok proceeded to implement and promote these features. Reportedly, TikTok also demoted people it deemed unattractive, was aware of harmful filter bubbles, and knew that its content moderation was sub-optimal. The Utah complaint reveals 'shocking findings' of an internal investigation conducted by TikTok into the LIVE feature. TikTok's spokesperson stated that the Kentucky and Utah complaints were cherry-picking misleading quotes and taking outdated documents out of context to misrepresent TikTok's commitment to community safety.

In the EU, TikTok has committed to permanently withdrawing its TikTok Lite Rewards programme, which came under scrutiny by the Commission under the DSA for its addictive effect. In a recent letter to Amnesty International, TikTok reiterated its youth protection measures including screen time limits, parental control features and reminders to switch off at night. Children can also experience positive health outcomes from using TikTok, such as finding community during COVID lockdowns or connecting with peers facing similar health challenges.

The EU legal framework

At the EU level, over 10 laws regulate social network operations.[9] These laws are not designed to address the identified risks on a one-to-one basis but follow a sectoral approach, pursuing different governance angles. Nevertheless, certain crosscutting themes align with specific risks. For instance, rules in the Unfair Commercial Practices Directive (UCPD), the GDPR and, as applicable, the Artificial Intelligence Act (AIA), relating to fairness and non-manipulation can be invoked to mitigate risks like addictive design and the exploitation of vulnerabilities. Given TikTok's popularity among minors who own smartphones – with 95 % using the app monthly, according to leaks from the Kentucky complaint – specific child protection rules apply.

Non-manipulation requirements

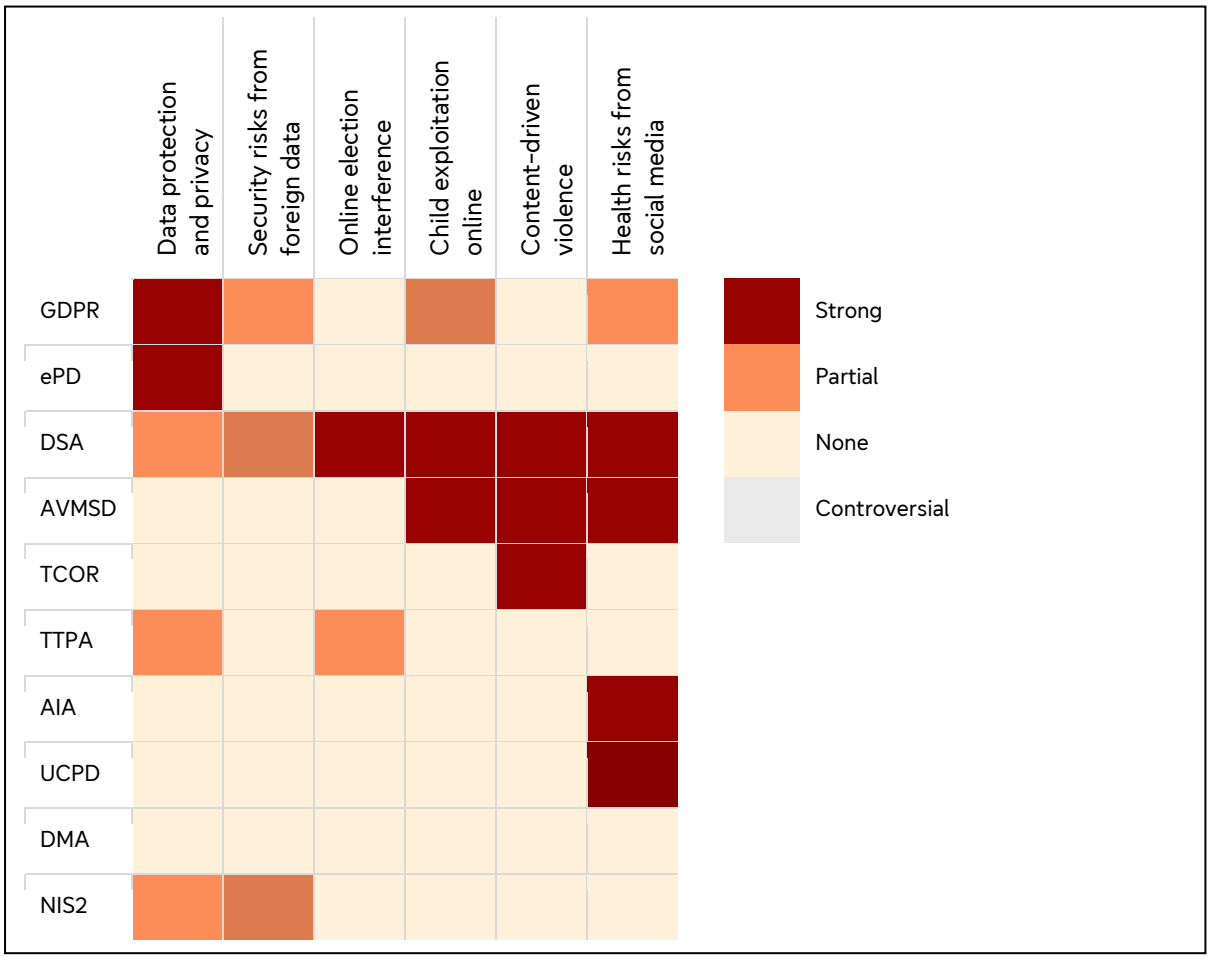
In the academic debate, social media platforms are linked to manipulation and the exploitation of vulnerabilities in different ways. Their algorithms may be the source of manipulation or users may use them as vehicles of manipulation. A precise definition of manipulation is still lacking. Provisions related to non-manipulation tie in with debates around user addiction, dark patterns, nudging, emotional and cognitive targeting, and deceptive disinformation.

With the inclusion of Article 5 in the AIA, the concept of non-manipulation has been given a prominent place in EU law. This rule prohibits AI systems that distort a person's behaviour in a significantly harmful manner by deploying subliminal or purposefully manipulative techniques, or by exploiting vulnerabilities. Most recently, the NGO SOMI filed multiple class actions against TikTok alleging that its addictive features violate the AI Act's prohibition of manipulative AI systems.[10] Conversely, common and legitimate advertising that complies with applicable laws does not qualify as an inherently harmful manipulative AI-enabled practice (Recital 29 AIA). This does not rule out a ban on cases of exploitative targeting or supercharged futuristic manipulation systems.

If Article 5 AIA fails to ban addictive AI systems of social media companies, then the AIA's overall effectiveness in mitigating related harms would be significantly limited. TikTok's contemporary content management systems would only be subject to obligations under the AIA if their systems were classified as high-risk AI under Annex III of the AIA. This would include AI systems designed to influence elections (e.g. political advertising targeting and delivery systems) or which use biometric data (e.g. recommender systems based on keystroke characteristics). In these scenarios, providers

are required to continually identify and mitigate foreseeable risks to health, safety, or fundamental rights (as outlined in Articles 9, 16(c) and 17(1)(g) AIA). There is currently no evidence to suggest that TikTok uses biometric data in its recommender systems. While TikTok's US privacy policy mentions the collection of biometric data, its EU privacy policy does not address such practices.

Figure 1 – The role of EU secondary legislation in addressing the key issues identified



Source: Author's own elaboration. The colour coding indicates a generalised assessment of the scenarios in the text.

Under the DSA, very large online platforms such as TikTok must assess and mitigate the risk of serious negative consequences to users' physical and mental wellbeing (including addiction risks) and foreseeable negative effects on civic discourse and electoral processes (Articles 34 and 35 DSA). Additionally, when delivering their services online, platforms must implement appropriate and proportionate measures to ensure a high level of privacy, safety and security for minors (Article 28 DSA). In line with the views expressed by academics, the Commission's draft guidelines on the protection of minors online under the DSA indicate that recommender systems and design features should not be optimised to maximise time spent and engagement. The DSA also prohibits online platforms from designing, organising, or operating their online interfaces in a way that deceives or manipulates the recipients or otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions (Article 25 DSA). In its 2024 risk assessment report, TikTok recognises a potential negative impact of increased screen time and social media use for younger users and mentions the mitigation measures it has adopted. As mentioned earlier in the section on public health risks, US attorneys general and Amnesty International question the effectiveness of these features.

Under the UCPD, the exploitation of cognitive errors through personalised advertising and addictive features may be considered unfair if it is likely to prompt the average consumer to 'click on a link or

advertisement online' or to 'continue using the service by browsing or scrolling'. Various academics argue that advertising targeted at emotional or cognitive weaknesses violates the UCPD's general clause or its prohibition of aggressive commercial practices. A similar argument has been made regarding addictive design. However, the Commission has recently suggested that this issue is more controversial than previously indicated in its guidance, and that it would depend on whether the UCPD's economic interest concept covers addictive design. Some stakeholders who responded to the Commission's public consultation on digital fairness believe that addictive design is new territory for EU consumer law.

Assuming the GDPR applies (Article 2(4) GDPR), data-driven systems entailing excessive risk of manipulative targeting could potentially violate the fairness principle, especially if the data collected is used against the data subject. The same could be said for data-driven recommender systems that lead to addiction. Additionally, platforms may face liability under contract and tort law, if aggrieved users can demonstrate that they suffered harms due to content-agnostic platform features or that contractual liability falls outside the scope of the DSA's content-liability exemption. In the US, academics and aggrieved individuals are increasingly questioning whether platforms should have broad immunity for all content-related platform features.

The AIA, the DSA, the GDPR and the Regulation on the transparency and targeting of political advertising (TTPA) contain additional rules that impose transparency requirements and profiling restrictions, thereby fostering accountability, hindering manipulative techniques and deterring individuals from using them (see sections on 'Fair data governance' and 'Transparency obligations').

According to the sector-specific Audiovisual Media Services Directive (AVMSD), video-sharing platforms such as TikTok may not use subliminal techniques in audiovisual commercial communications (Article 28b(2) and 9(1)(b) AVMSD).

Content stewardship requirements

Among other things, the DSA aims to mitigate various risks related to the dissemination and moderation of content. These risks include threats to due process, physical and mental well-being, electoral processes, public security and fundamental rights. The Act imposes asymmetric obligations on intermediary services, depending on their type and size. Very large online platforms (VLOPs) such as TikTok are subject to extensive rules, which include fair moderation processes, fair application and enforcement of content restrictions, risk-management duties, fair design obligations, and transparency and oversight rules.

Social media providers are generally exempt from liability for illegal content stored on their services, unless they fail to act promptly after becoming aware of it (conditional liability exemption). This exemption means they are not held liable for user-shared content such as CSAM or hate speech, unless they fail to take swift action upon being informed. In general, social media providers are not required to automatically detect and remove illegal content from their platform, but they must implement effective notice and action mechanisms along with complaint procedures. According to Article 28(1) DSA and Article 28b(1)(a) AVMSD, platforms must safeguard minors, which could involve measures related to the design of the recommender system and the organisation of content (Article 28b(1)(3) AVMSD).

VLOPs, such as TikTok, must also assess and mitigate systemic risks such as the dissemination of illegal content, negative effects on the exercise of fundamental rights, negative effects on electoral processes, and the ways in which the design and functioning of their services contribute to these risks (Article 34 and 35 DSA). The assessment should also analyse any intentional manipulation of their service, including inauthentic use or automated exploitation of the service, as well as the amplification and potentially rapid and wide dissemination of illegal and violative content (including through the use of bots or fake accounts). Mitigation measures may include adapting aspects of the provider's work, such as terms and conditions, the functioning of their service, content moderation processes, algorithmic systems (including recommender systems) and advertising systems, as well as ensuring that false information is marked. Some academics argue that the Commission's power

in reviewing mitigations measures depends on whether the content is illegal or 'lawful but awful'. Where content is legal, the Commission must refrain from demanding content-specific restrictions and must remain content-neutral. This could 'involve empowerment of users, or redesign expectations that apply to services in general, such as circuit breakers, limits on authentic behaviour or super-users'.

The Commission's first risk-related DSA guidelines focus on safeguarding the integrity of elections. After receiving reports of Russian interference in the Romanian elections through TikTok, the Commission initiated formal proceedings against TikTok in December 2024.

Cybersecurity requirements

It is unclear whether EU cybersecurity rules prevent providers from voluntarily sharing user data with foreign affiliates who may be forced to pass it on to their governments. Providers of social networking services platforms such as TikTok may qualify as important entities under the Network and Information Security Directive (NIS2). As such, they would need to implement appropriate and proportionate technical, operational and organisational measures to manage the risks to the security of network and information systems used to provide their services. While the Commission's Implementing Regulation on cybersecurity risk-management measures addresses unauthorised access and the misuse of access rights, it does not address situations where a company willingly grants a foreign affiliate access to user data. Without a mechanism to designate a country as a foreign adversary country, it is challenging to see how these rules could be used to prevent such access unless, for example, the data sharing clearly facilitates an attack on the network and information system. A similar argument can be made regarding the cybersecurity provisions under the AIA and the GDPR. However, the GDPR's data transfer rules can block such transfers (see Section on 'Data protection and privacy' above).

If data storage and access management qualify as function-driven risks under Article 34 DSA, TikTok would have to mitigate public security and data protection risks arising from sharing data with foreign affiliates according to Article 35 DSA. In case of non-compliance, the Commission can prescribe interim measures, adopt a non-compliance decision and impose fines. The Commission spokesperson has stated that the suspension of TikTok is a competence of the national authorities. Within the DSA, suspension would be a last-resort measure that is only available in case of a serious threat to the security of citizens. However, the spokesperson emphasised that it is not the Commission's objective to suspend any platform in the EU and that there are proportionate sanctions foreseen in the DSA. In this context, it is worth recalling that the Commission suspended TikTok from corporate devices in February 2023, and this decision is still in force.

Crosscutting risk mitigation requirements

Many digital regulations establish broad risk management duties. It is important to underline that the risk management duties of VLOPs under the DSA do not only concern content-related risks but also risks stemming from the overall design and functioning of the platform's service. Under the AIA, providers of high-risk AI systems must set up a quality management system. Due to the closed – but amendable – list of high-risk AI systems in Annex III, the obligation only applies to a narrow set of systems used by social media, as mentioned earlier on in this briefing. Insofar as social media platforms integrate general-purpose AI (GPAI) models with high-impact capabilities, such as ChatGPT-4, they would have to assess and mitigate possible systemic risks (Article 55(1)(b) AIA). Both the AIA and the DSA require that the risk of misuse be taken into account.

According to Article 35 GDPR, data controllers must also perform a data protection impact assessment when the processing of personal data is likely to pose a high risk to individuals. The impact assessment must evaluate the risks to the rights and freedoms of natural persons, focusing on data protection and privacy, as well as freedom of speech, freedom of thought, prohibition of discrimination, and the right to liberty, conscience and religion (Article 35(7b) GDPR). To avoid

having to consult the supervisory authority, data controllers must address any high risks prior to processing the data (Articles 25, 35(7)(d) and 36 GDPR).

Fair data governance requirements (including profiling)

The GDPR applies to the way TikTok operates, as the platform's use involves processing of behavioural data and personal data contained in user-generated content. Following the main legal principles of data protection, data processing must be lawful, fair and transparent; have a specific, explicit and legitimate purpose; and comply with the requirements of data minimisation, data accuracy, storage limitation, data security and accountability (Article 5 GDPR). In addition to ensuring all of this, TikTok must obtain consent for the storage of tracking cookies under the e-Privacy Directive. As detailed in the Section on 'Data protection and privacy' above, TikTok has been the subject of a range of sanctions and complaints.

Additionally, the DSA, the Digital Markets Act (DMA) and the TTPA impose restrictions on data processing and profiling practices that may affect the accuracy of targeted messaging and content dissemination. Individuals that platforms reasonably believe to be minor or younger than one year below the voting age benefit from enhanced protection from targeting based on profiling using personal data or even based on the processing of personal data in general.

Transparency obligations

The applicable laws contain a plethora of transparency requirements designed to foster responsible behaviour through corporate accountability, safeguard rights, increase transparency within industries, ensure effective access to justice and build trust in new technologies.

Conclusion

This review shows that regulatory authorities have wide-ranging enforcement powers that can be used to address the key issues identified. While compliance measures may well spark geopolitical tensions, it is worth noting that China has banned many Western social media platforms ('The Great Firewall') and has taken radical measures[11] to protect its youth from internet addiction and other risks. Tensions could be eased by cooperating on shared priorities (such as child protection), avoiding misleading narratives on initiatives and actions (such as regarding the legal effects of the DSA), respecting each other's digital sovereignty, fostering strategic and operational interdependence, and exploring privacy-enhancing middleware solutions.

There is room to enhance legal certainty and protection, for instance, through guidelines or regulations. The European Commission is currently assessing the fitness of the legal framework and advocating for a digital fairness act, a European democracy shield, and a regulation combating child sexual abuse online. Some Member States advocate for built-in age verification, a European Digital Majority Age, and age-appropriate design. With the entry of Chinese 5G infrastructure, electric vehicles and applications such as TikTok, discussions on the EU's security may reignite in the near future. The rationale and evidentiary standard underpinning new policies can vary. The US Supreme Court held in its judgement on the TikTok ban that 'Sound policymaking often requires legislators to forecast future events and to anticipate the likely impact of these events based on deductions and inferences for which complete empirical support may be unavailable'. Additionally, policymakers could bring forth arguments about the negative impacts on overall net welfare, emphasise shared social responsibilities, and invoke the principle of the cheapest cost-avoider.

ENDNOTES

[1] The figures for Google and Meta cover revenues from a variety of products. Additionally, revenues are not necessarily channelled through the companies located in the regions where the ads are delivered. Even if this were the case, user location is estimated based on different factors such as geographical locations or the address which they registered when signing up to the service.

[2] Reportedly, TikTok had previously used this system to collect and retain personal data of US users who watched LGBTQ+ content and users who expressed views on gun control, abortion, and religion.

[3] According to information from another context, Lark had a 'secure messaging' and 'recall' feature, which enabled (certain) TikTok employees to send disappearing chats and overwrite messages. Metadata or audit logs were not available. The House Committee on Energy and Commerce collected public statements on TikTok's national security risks.

[4] CJEU case law makes it clear that foreign laws and practices concerning indirect government access to user data (including for national security) must be considered when assessing data protection adequacy prior to international transfers.

[5] See the judgments, the 2025 annual threat assessment of the US Intelligence Community, and the 2024 annual report of the Congressional-Executive Commission on China.

[6] As of 2022, that committee 'was headed by the company's chief editor and comprised at least 138 employees'.

[7] K. Müller and C. Schwarz, 'Fanning the Flames of Hate: Social Media and Hate Crime', *Journal of the European Economic Association*, Vol. 19(4), 2021, pp. 2131-2167; K. Müller and C. Schwarz, 'From Hashtag to Hate Crime: Twitter and Antiminority Sentiment', *American Economic Journal: Applied Economics*, Vol. 15(3), 2023, pp. 270-312; M. Bozhidarova et al., 'Hate speech and hate crimes: a data-driven study of evolving discourse around marginalized groups', *2023 IEEE International Conference on Big Data (BigData)*, pp. 3107-3116; C. Arcila Calderón et al., 'From online hate speech to offline hate crime: the role of inflammatory language in forecasting violence against migrant and LGBT communities', *Humanities and Social Sciences Communications*, Vol. 11(1), Article No 1369; M. Popa-Wyatt, 'Online Hate: Is Hate an Infectious Disease? Is Social Media a Promoter?', *Journal of Applied Philosophy*, Vol. 40(5), 2023, pp. 788-812.

[8] California, New York, Illinois, Kentucky, Louisiana, Massachusetts, Mississippi, North Carolina, New Jersey, Oregon, South Carolina, Vermont, Washington, and the District of Columbia. Subsequently, the AG of Virginia and Alabama also filed a lawsuit. The attorneys general of Utah [2023 and 2024], Nevada, Indiana, New Hampshire, Nebraska, Arkansas, Iowa, Kansas, and Texas had already filed prior actions against TikTok for its conduct toward youth. Additionally, AGs have filed lawsuits for TikTok misrepresenting the risk of Chinese data access.

[9] These include – as applicable – the non-discrimination directives, the GDPR, the ePD, the UCPD, the UCTD, the DSA, the AVMSD, the CSAR (applicability to chat features being uncertain), the TCOR, the EMFA, the TTPA, the AIA, the NIS2 and the DMA.

[10] It can be argued that the underlying AI system should not be assessed in isolation from the user-facing application components that it powers. A well-designed platform without an effective recommender system would hardly attract users and the scroll-on functionality relies on a steady stream of personalised content. Alternatively, the focus could be limited to the recommender system's optimisation for engagement (in a specific design environment).

[11] In 2007 China included the concept of 'internet addiction' in its Law on the Protection of Minors, and in 2021 it included a chapter on 'internet protection', obliging social networks to protect the youth against internet addiction (see Article 74 et seq.). Most recently, the State Council adopted an order, which took effect on 1 January 2024 and included a chapter on the prevention of internet addiction. On November 15, 2024, the Cyberspace Administration of China (CAC) released its 'Guidelines for the Construction of Mobile Internet Mode for Minors'.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

https://eprs.in.ep.europa.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)

Annex: Selected evidence on the effects of social media on adolescent health

Public sector organisations, academics and practitioners have identified connections between social media use and a range of adverse outcomes – including physical and mental health issues such as sleep deprivation, eating disorders, depression and anxiety. Negative psychological experiences such as reduced self-esteem resulting from social comparison have also been linked to excessive or otherwise problematic social media use, along with poor concentration, mood issues and increased risks of loneliness and suicidal tendencies. Social media are considered particularly harmful to girls. Some researchers view the cross-sectional evidence as inconsistent and inconclusive, as studies vary in the methods they employ, apply different levels of rigour and face potential confounding factors. However, small to moderate associations have been observed. Nevertheless, even those who challenge causal claims suggest that social media might amplify the developmental changes that increase adolescents' mental health vulnerability, warranting further analysis. Additionally, platform design can exploit existing psychological biases and encourage habitual social media scrolling, posting and sharing. It is also acknowledged that time spent on social media increases the risk of alcohol, e-cigarette and tobacco use in adolescents. Parliamentary committees across the world have collected a wealth of evidence on the health risks of social media.

Reports from public sector organisations

- S. Galea et al. (eds), Social Media and Adolescent Health, Consensus Study Report, National Academies of Sciences, Engineering and Medicine, 2024;
- US Surgeon General, Social Media and Youth Mental Health, The US Surgeon General's Advisory, 2023;
- (Interagency) Kids Online Health and Safety Taskforce, Online Health and Safety for Children and Youth: Best Practices for Families and Guidance for Industry, Output report, 2024;
- M. Boniel-Nissim et al., A focus on adolescent social media use and gaming in Europe, central Asia and Canada, World Health Organization, 2024;
- European Commission's Joint Research Centre (JRC), The JRC explains: Why are children and adolescents vulnerable to social media?, JRC website, 18 March 2025;
- E. Young et al., 'Frequent Social Media Use and Experiences with Bullying Victimization ...', Center for Disease Control's *Morbidity and Mortality Weekly Report*, 2023, Vol. 73(4), pp. 23-30;
- UK Commons Select Committee on Education, Screen time: impacts on education and wellbeing, 4th report of Session 2023-24, 2024;
- UK Commons Select Committee on Science, Innovation and Technology, Impact of social media and screen-use on young people's health, 14th Report of Session 2017-19, 2019;
- Office of the Minnesota Attorney General Keith Ellison, Minnesota Attorney General's Report on Emerging Technology and Its Effects on Youth Well-Being, Report at the request of the Legislature, February 2024;
- AU Joint Select Committee on Social Media and Australian Society, Social media: the good, the bad, and the ugly, Final report, November 2024;
- B. O'Neill, The influence of social media on the development of children and young people, Directorate-General for Internal Policies of the Union (IPOL), European Parliament, 2023.

Parliamentary inquiries and hearings

- EP Committee on Women's Rights and Gender Equality (FEMM), Social media and the consequence on young girls' mental health, Hearing, 28 January 2025;

- US Senate Committee on the Judiciary, Protecting Our Children Online, Hearing, 14 February 2023;
- UK Commons Select Committee on Science, Innovation and Technology, Impact of social media and screen-use on young people's health, Inquiry, 2018-2019;
- UK Commons Select Committee on Education, Screen Time: Impacts on education and wellbeing, Inquiry, 2023-2024;
- Australian Joint Select Committee on Social Media and Australian Society, Inquiry into Social Media and Online Safety, starting 16 May 2024 (hearings listed in Appendix 2);

Studies and reviews by academics and practitioners

- M. Prinstein, Written testimony for the Senate Committee hearing on Protecting Our Children Online, American Psychological Association, 2023;
- A. Kaur Purba et al., Written evidence submitted by the Digital Mental Health Programme at the University of Cambridge, SMH0027, Commons' Committee hearing on Social media, misinformation and harmful algorithms, 2024;
- M. Griffiths et al., Written evidence submitted by International Gaming Research Unit, Nottingham Trent University, SMH0091, Commons' Committee hearing on Impact of social media and screen-use on young people's health inquiry, 2018;
- C.S. Andreassen, 'Online Social Network Site Addiction: A Comprehensive Review', *Current Addiction Reports*, Vol. 2, 2015, pp. 175-184;
- H. Allcott et al., 'Digital Addiction', *American Economic Review*, Vol. 112(7), 2022, pp. 2424-2463;
- L. Braghieri et al., 'Social Media and Mental Health', *American Economic Review*, Vol. 112(11), 2022, pp. 3660-3693;
- J. Haidt, The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness, Penguin Press, 2024;
- J. Haidt, et al. (ongoing), Social media and mental health: A collaborative review, unpublished manuscript, New York University, last accessed 9 April 2025;
- A. Lembke, Applying the Bradford Hill Criteria to Social Media Use and Adolescent Mental Health, After Babel blog, 2024.

Flavour of the debate surrounding causal claims

a) Critical voices:

- A.K. Przybylski et al., Written evidence submitted by Professor Andrew K Przybylski, Netta Weinstein, and Amy Orben, SMH0140, Hearing on Impact of social media and screen-use on young people's health, 2018;
- A. Orben, Written Evidence Submitted by the Digital Mental Health Research Group, University of Cambridge, ST0022, Hearing on Screen Time: Impacts on education and wellbeing, 2023;
- A. Orben et al., 'Windows of developmental sensitivity to social media', *Nature Communications*, Vol. 13, 2022, Article No 1649;
- A. Orben & S.-J. Blakemore, 'How social media affects teen mental health: a missing link', *Nature*, Vol. 614, 2023, pp. 410-412;
- C.L. Odgers, 'The great rewiring: is social media really behind an epidemic of teenage mental illness?', *Nature*, Vol. 628, pp. 29-30;
- C. Ferguson, Social Media...Again...Ugh..., Secrets of Grimoire Manor blog, October 2024.

b) Responses:

- J. Haidt, Yes, Social Media Really Is a Cause of the Epidemic of Teenage Mental Illness, After Babel blog, 2024;
- J. Haidt, Why Some Researchers Think I'm Wrong About Social Media and Mental Illness, After Babel blog, 2023;
- D. Stein, Nature's Review of The Anxious Generation Part 1, Part 2, Part 3, The Shores of Academia blog, 2024;
- D. Stein, Unjustified Critique of a CDC Report on Social Media Risks, The Shores of Academia blog, 2024.