TAXPAYERS PROTECTION ALLIANCE

September 1, 2025

The Honorable Scott Fitzgerald
Chair, Subcommittee on the Administrative State, Regulatory Reform, and Antitrust
Committee on the Judiciary
U.S. House of Representatives
2138 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jerrold Nadler
Ranking Member, Subcommittee on the Administrative State, Regulatory Reform, and Antitrust
Committee on the Judiciary
U.S. House of Representatives
2141 Rayburn House Office Building
Washington, D.C. 20515

Re: September 3, 2025, Hearing Entitled "Europe's Threat to American Speech and Innovation"

Dear Chair Fitzgerald, Ranking Member Nadler, and Members of the House Judiciary Committee Subcommittee on the Administrative State, Regulatory Reform, and Antitrust,

We won the Revolution; let's not lose the peace.

In the digital age, technology transcends borders. Platforms created in Silicon Valley connect users worldwide, allowing people in Melbourne (Australia) to read the opinions of users in Stockholm (Sweden) or customers in Toronto (Canada) to buy the products of entrepreneurs in Cape Town (South Africa). Likewise, a regulation of technology often transcends the borders of the jurisdiction that enacts it. As American tech companies have learned, policies enacted in faraway Europe have staggering consequences here at the United States. Two such policies are the European Union's (EU) Digital Markets Act (DMA)[1] and the Digital Services Act (DSA).[2] Both impose extensive regulatory burdens on covered platforms, most of which are American in origin.[3]

The extension of European-style regulation to U.S. technologies should trouble policymakers. The respective approaches of the two jurisdictions have resulted in wildly different outcomes. With relative freedom, American innovators have made the U.S. tech sector the best and the envy of the world. On a list of the largest tech companies, America claims the first seven spots, 11 of the first 15, and 19 of the first 25.[4] It is not until one goes 15 slots down the list that one encounters a firm from the EU (Germany's SAP). Having tightened the regulatory vice and squeezed every ounce of dynamism out of its own—preventing a robust continental tech sector from ever having been developed—Europeans now seek to impose the same kind of smothering technocratic micromanagement of technology on the American firms on which European businesses and users have come to rely.

EU tech policy has already begun to arrive in the U.S. Europe's immense market power and the inherently international nature of digital markets extend its regulatory reach beyond its jurisdiction. American consumers felt the EU's touch when, to comply with EU privacy law, websites began to display cookie-consent boxes.[5] Another European mandate strong-armed Apple to transition its iPhones to the USB-C charger.[6]

The faults of the DMA and DSA are no longer theoretical; they are documented in empirical evidence. American policymakers—including this Subcommittee—should be commended for taking note.

American companies and American users have found themselves subject to "the Brussels effect." Due to the EU's regulatory might and the size of its population, it often enjoys the ability to affect policies and markets far beyond its jurisdiction. This cannot be tolerated, particularly given the European aversion to free markets and free speech, two cornerstones of the American political tradition. Nowhere are the differences between Americans and the rest of the world seen with more clarity than in the tech sector.

[1] https://digital-markets-act.ec.europa.eu/index_en
[2] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
[3] https://www.protectingtaxpayers.org/technology/hypocrisy-thy-name-is-europe/
[4] https://companiesmarketcap.com/tech/largest-tech-companies-by-market-cap/
[5] https://www.nationalreview.com/2024/07/europe-would-rather-regulate-tech-than-innovate/
[6] https://www.bloomberg.com/news/newsletters/2023-09-03/apple-september-12-event-iphone-15-charging-port-change-to-usb-c-from-lightning-lm3gn2hs

America has put its trust in freedom; the Europeans, in technocracy. The tech sector of the former has flourished; that of the latter has withered. The mistakes that have festered in the Old Europe must not be foisted on the United States.

The Digital Markets Act

The DMA is a sprawling and complicated regulation designed to allow regulators to control the minutiae of many types of online commerce. A few high-level failings stand out.

The law creates a sweeping and unbending list of obligations and prohibitions that governs ten categories of economically significant "gatekeeper" platforms. Examples include operating systems, search engines, web browsers, social-media platforms, and more. However, many newly forbidden business practices have generally pro-competitive or pro-consumer effects. "The prohibited practices are presumed to harm competition irrespective of efficiency considerations raised by the [business], such as improving consumer welfare or product improvement by technological innovation," explains Aurelien Portuese, now a professor and the founding director of the GW Competition & Innovation Lab at The George Washington University.[7] Any market hobbled by such inflexibility will invariably produce fewer innovative products and business strategies. This will further smother Europe's already lagging tech sector—as well as regulated American tech firms.

Then there is the DMA-proscribed practice of "self-preferencing," whereby a search engine or online marketplace prominently features its own products. For example, Google Search "preferences" Google Maps over other mapping services. Another instance is Amazon's search results, which promote the marketplace's in-house product lines, such as Amazon Basics. In both cases, consumers benefit. Google Maps' prominent search positioning spares users the time that would be required to wade through a list of mapping services simply to find directions. Likewise, Amazon's self-preferencing highlights affordable products with a familiar brand they can rely on. If consumers don't want either of those, they can continue scrolling as normal.

Moreover, despite the agitation of pro-DMA technocrats, self-preferencing often benefits large platforms' small competitors. "Platforms that preference their own products frequently end up increasing the total market's value by growing the share of users of a particular product," writes Dirk Auer, director of competition policy at the International Center for Law & Economics.[8] "Those that preference inferior products end up hurting their attractiveness to users of their 'core' product, exposing themselves to competition from rivals."

The DMA further fails to account for the nuances of market share. A dominant incumbent in one market may be a disrupter in another. Apple is the premier programmer and manufacturer of mobile phones, but it is just another competitor in the streaming market.[9] Nonetheless, "the DMA will regulate Apple Music (which has 15 percent market share) while exempting Spotify (31 percent market share)," Portuese notes. This is transparent protectionism for the European-owned Spotify against American competition. This is contrary to DMA proponents' claims of safeguarding market competition.

Such shortsightedness stretches across many industries. "In the travel industry, the DMA will impose restrictions on Google Flights while exempting such incumbents as Expedia," Portuese continues. "Within the social media industry, the DMA will regulate Facebook while exempting Twitter."

Looking back, the General Data Protection Regulation's (GDPR) regulatory heavy-handedness reduced app availability, measured on the Google Play app store, by a third.[10] It also slowed the rate at which new apps appeared by nearly half. Looking forward, the Center for Strategic and International Studies (CSIS) estimates regulatory costs associated with the DMA and DSA could reach $70 billion for European companies alone (about 0.3 percent of EU GDP).[11] Further, American firms could, conservatively, see an invoice of $50 billion, CSIS says. These laws are not a formula for innovative dynamism and consumer choice. And, like any new tax or regulation on business, these costs will ultimately be borne by consumers. Those costs include delayed or altogether forgone access to digital

[7] https://itif.org/publications/2022/08/24/digital-markets-act-a-triumph-of-regulation-over-innovation/
[8] https://truthonthemarket.com/2022/01/18/10-things-the-american-innovation-and-choice-online-act-gets-wrong/
[9] https://www.businessofapps.com/data/music-streaming-market/
[10] https://www.nber.org/system/files/working_papers/w30028/w30028.pdf
[11] https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-02/221122_EU_DigitalRegulations-3.pdf?VersionId=04r7zBzS2kHNhsISAqn4NkC6lGNgip7S

products. For example, Apple delayed access to European users to its artificial intelligence (AI) tool, Apple Intelligence, citing DMA regulations as the reason.[12]

The defects of the DMA's enforcement are bad enough—yet the law's enforcement caused still more damage. The law provides enforcers with wide discretionary latitude, ensuring companies lack any reasonable means to determine what businesses' practices will attract scrutiny. To comply with the DMA, Meta initiated a "pay or consent model," allowing Facebook and Instagram users to opt out of data gathering for a monthly fee.[13] The costs of this kind of enforcement are staggering. Meta changed its policy in an attempt to comply, but the European apparat, unsatisfied with the new choice given to users, invented a dubious application of the law to continue its crusade against the American tech giant—a "violation" that carried a €200 million fine. This sort of arbitrary enforcement creates an unfriendly climate for business and innovation, the results of which are manifest in Europe's puny tech sector.

The DMA also threatens users' cybersecurity. EU officials promote the law as a pro-consumer, pro-competitive measure. However, the DMA will harm both consumers and competition. Its mandates will harden the regulatory flexibility that thus far has promoted the constant innovation to which the digital age owes its excellence.

The EU's purported intention to promote consumer choice deserves credulous scrutiny. Many consumers prefer closed and integrated platforms and tech ecosystems, which often offer conveniences[14] and security features.[15] The DMA gainsays many such choices, prescribing which consumer-chosen features tech companies may continue to offer.

In March 2024, Apple published a paper that examines how the DMA will change its products with respect to privacy and cybersecurity. Apple's comparatively tight technical controls, which are undergoing significant changes to comply with the DMA, make it a particularly notable gatekeeper platform. For example, iOS (Apple's operating system) devices thus far have barred users from downloading apps outside the vetted App Store. The DMA compels operating systems to allow this process, called "sideloading," despite its inherent cybersecurity risks.[16]

By fiat, Europe has materially degraded its citizens' cybersecurity. As the Apple report acknowledges, "the changes the DMA requires will inevitably cause a gap between the protections that Apple users outside of the EU can rely on and the protections available to users in the EU moving forward."

Even European government agencies recognize the dangers of sideloading. "Government agencies, both in the European Union and outside of it, have been quick to recognize the risks created by these new distribution options and the need for protective measures," Apple says. "These agencies…have reached out to us about these new changes, seeking assurances that they will have the ability to prevent government employees from sideloading apps onto government-purchased iPhones."

The alarm is being rung even by some Europeans.[17] Benedikt Franke (the vice-chairman and CEO of the Munich Security Conference) argues that "that regulations and policies seeking to address new realities need to be 'security proofed' before they're passed."[18] The DMA, he writes, fails to meet this standard. "[T]here's plenty of evidence that it comes with serious side effects, putting millions at risk by overriding central safeguards on the pretense of consumer choice," he states.

Digital platforms, digital systems, and digital consumer protections have evolved over the course of the last decades in an iterative process of determining what contours are necessary for tech companies to innovate revolutionary products and what features consumers prefer. The DMA attempts to eliminate this process of discovery and replace it with the prescriptive, arbitrary, and subjective preferences of European officials. Allowing this to go forward unchallenged will make the internet a poorer, less dynamic,

[12] https://townhall.com/columnists/david-b-mcgarry/2024/07/22/how-europe-is-breaking-the-internet-n2642013
[13] https://www.theverge.com/2024/7/1/24189796/eu-meta-dma-violation-pay-consent-ads-model
[14] https://www.nationalreview.com/2022/07/the-bipartisan-antitrust-bill-is-a-dangerous-mistake/
[15] https://www.nationalreview.com/2023/05/digital-antitrust-poses-a-security-hazard/
[16] https://appsecurityproject.org/issues/mandated-sideloading-will-weaken-the-app-ecosystem-and-compromise-existing-privacy-protections/
[17] https://appsecurityproject.org/news_post/european-security-expert-calls-out-digital-markets-act/
[18] https://www.politico.eu/article/its-time-to-security-proof-europes-tech-policies/

and less safe place—likely both for Europeans and for Americans. It will also slow the pace of innovation in an industry that is at the forefront of economic growth and innovation.

The Digital Services Act

The DSA inflicts on free speech the damage the DMA inflicts on markets and digital platforms. For all its power, technology cannot rid the world of disagreement and, in many circumstances, falsehood. Bad information is endemic to the human condition and to human interaction in two senses. First, perception and reason are fallible, even if unclouded by interest or passion. Never yet was the person born whose opinions were not in some way faulty. Mistakes and inaccuracies will, therefore, be committed—online and offline, both.

Second, those who set themselves up as censors are—like everybody else—imperfect. The definitions of disinformation and misinformation—let alone malinformation—often extend to information that cannot, in any objective sense, be considered false. The theory of COVID-19's likely origin in a lab in Wuhan, China migrated from a conspiracy to likelier-than-not over a few months; yet in the interim, analysts who propounded and offered evidence for this theory were maligned as quacks. Put differently, charges of disinformation are often leveled by the censorious to skirt the critical truth-seeking process of debating contentious and uncertain issues of national import.

In 1644's Areopagitica, John Milton questioned the notion that censors will light upon the truth. "It cannot be denied but that he who is made judge to sit upon the birth or death of books, whether they may be wafted into this world or not, had need to be a man above the common measure, both studious, learned, and judicious," Milton wrote of England's book-licensing code; "there may be else no mean mistakes in the censure of what is passable or not; which is also no mean injury." Milton's warning holds true today. When authorities undertake to declare some opinion true and others false, and so to dispense with further argument, they will invariably err. Despite all this, many seek to render the internet free of inaccuracy and (subjectively) objectionable speech. In a recent interim staff report, the House of Representatives Judiciary Committee documents the DSA's efforts to censor online information that European officials disapprove of.

The mechanisms of the DSA's censorship include:

- "Article 21 mandates that platforms allow certified third-party arbitrators to resolve content moderation disputes. These arbitrators must be independent from the platforms, but do not need to be independent from the European regulators who certify them, incentivizing arbitrators to heed regulators' censorship demands."
- "Similarly, DSA Article 22 requires that platforms give priority to censorship requests from government-approved third parties known as 'trusted flaggers.' In practice, these trusted flaggers are uniformly pro-censorship, and in many cases, they are government-funded, meaning that these so-called 'trusted' flaggers are incentivized to censor speech critical of politicians or the current regime."
- "The core of the DSA is the risk assessment and mitigation framework set out in Articles 34 and 35. These provisions encourage platforms to censor a wide variety of speech. Tech companies are directed to identify 'systemic risks' present on their platforms, which are defined to include 'misleading or deceptive content,' 'disinformation,' 'any actual or foreseeable negative effects on civil discourse and electoral processes,' and 'hate speech.' Platforms are specifically warned that this systemic risk may include 'information which is not illegal.' Then, under the DSA, platforms must mitigate these risks, meaning they ultimately must remove content that European regulators deem 'misleading,' 'deceptive,' or 'hate[ful].'"

The DSA does not merely interpose between users and the kinds of speech that the First Amendment does not protect. Quite the contrary: "Documents produced to the Committee under subpoena show that European censors at the Commission and member state levels target core political speech that is neither harmful nor illegal, attempting to stifle debate on topics such as immigration and the environment," Judiciary relates. For example, Polish authorities flagged a post for stating that "electric cars are neither ecological nor an economical solution."

Efforts to rid the internet of officially disfavored speech will end not only in violations of users' right to free speech but in a shrunken, impoverished internet, bereft of truth. Classical sources liken truth to light; under the regime of the DSA—and other laws like it—the online world has become a far darker place.

It should be noted that Europe, generally speaking, has far less regard for free speech than do Americans. Says Dr. Matthäus Fink, a German prosecutor who enforces hate speech laws: "They don't think it was illegal. And they say, 'No, that's my free speech.' And we say, 'No, you have free speech as well, but it … also has its limits.'" Those limits have been found by the roughly 750 defendants Fink says his unit has convicted of online speech "crimes."[19]

Within Europe's boundaries, the prosecuted include: a German man who referred to a politician as an anatomical vulgarity;[20] an American in Germany who employed a swastika as a rhetorical device to criticize the country's COVID-19 policies;[21] and myriad other cases.[22] Politicians have—all too predictably—exploited censorship laws. "Robert Habeck, a leader of the [German] Green Party, has initiated over 800 criminal complaints since taking up his position as vice chancellor in 2021," writes Yascha Mounk.[23]

American Policymakers Should Resist the EU's Regulatory Overreach

American policymakers should resist the encroachments of the DMA and DSA on American tech companies. Currently, the choice faced by regulated platforms is either to comply with onerous anti-innovation, anti-consumer, anti-market, and anti-speech regulation or to withhold services from the continent. Despite the damage that might flow from compliance, the size and population of the EU render the latter option infeasible.

This does not mean, however, that the situation is hopeless. Recent efforts by the Trump administration have proven effective in rolling back bad tech policy on the Eastern side of the Atlantic Ocean.

In the U.K., regulators have worked to compromise—if not mortally wound—user privacy. Despite its departure from the EU, the U.K. has also embarked on a dangerous and anti-consumer tech policy.[24] In January, a U.K. agency ordered Apple to provide officials access to encrypted cloud-stored user data. Not content merely to snoop on its own citizens, the officials also seek access to the data of not just U.K. citizens but of users worldwide. To be quite clear, without secure encryption, users lose a substantial degree of privacy. Once flung open, such "backdoors" to encrypted data become accessible to cybercriminals as well as law enforcement. Moreover, granting the government indiscriminate access to all digital data would vitiate the principles of privacy and protection from wanton state snooping—principles that, while embodied in the Fourth Amendment, originated in the English legal tradition.

Apple challenged the order and, in the interim, withheld the affected services from U.K. users.

Now, according to the Financial Times, U.K. regulators are in retreat.[25] Unnamed senior U.K. officials say that President Donald Trump's administration—notably Vice President JD Vance—has resisted the January order and seems poised to have its way. "This is something that the vice-president is very annoyed about and which needs to be resolved," an official told the Financial Times. "The Home Office is basically going to have to back down."

Vance's campaign seems to have found success.[26] "[T]he U.K. has agreed to drop its mandate for Apple to provide a 'back door' that would have enabled access to the protected encrypted data of American citizens and encroached on our civil liberties," Director of National Intelligence Tulsi Gabbard announced recently.[27] This proof of concept—demonstrating the capacity of the U.S. government to resist and roll back foreign regulatory overreach—ought to fortify the confidence of the Trump administration as it seeks to make international tech markets (relatively) free and preserve the civil liberties of American users.

[19] https://www.cbsnews.com/news/germany-online-hate-speech-prosecution-60-minutes/
[20] https://www.cbsnews.com/news/germany-online-hate-speech-prosecution-60-minutes/
[21] https://www.thefire.org/news/american-writer-living-germany-could-face-jail-time-using-satirical-swastika-voice-dissent
[22] https://www.thefire.org/news/60-minutes-and-vice-president-vance-put-europes-worrying-speech-restrictions-spotlight
[23] https://yaschamounk.substack.com/p/europe-really-does-have-a-free-speech
[24] https://www.nationalreview.com/2025/03/what-american-lawmakers-should-learn-from-europes-newest-tech-policy-blunders/
[25] https://www.ft.com/content/3a3e6dbc-591d-4087-9ad3-11af04f0176f
[26] https://www.washingtonpost.com/technology/2025/08/19/uk-apple-backdoor-data-privacy-gabbard/
[27] https://x.com/DNIGabbard/status/1957623737232007638

The same sort of pressure ought to be brought to bear on European officials over the DMA and the DSA. Since foreign policy is primarily the province of the executive branch, the question is raised regarding what Congress—and this Subcommittee—can do to aid these efforts.

First, it is an evergreen statement that, in the American constitutional system, Congress is the first branch of government and the branch that first and foremost determines the federal government's policy. Congress should act to direct the President to resist foreign tech-policy abuses that objectionably target American companies and threaten American users. Doing so would allow Congress to determine the tone—and, to a large degree, shape the content—of these efforts. Moreover, although the Trump administration deserves praise for its efforts to this point, there is a meaningful difference between a self-directed diplomatic campaign and the execution of statutorily defined duties with a set of statutorily defined powers.

Conclusion

Never has the time been better—and never has it been more urgent—for American policymakers to counter the anti-American tech policy that has characterized decades of EU regulation. This regulation has been anti-American in two senses: it contravenes American principles, and it threatens the freedom and prosperity of American tech companies and American citizens. TPA applauds the Subcommittee for its attention to this critical matter. Commonsense legislation to empower and direct the President to engage in diplomacy to reverse the overreaches of the DMA and DSA would represent a salutary effort to protect Americans from foreign regulatory depredations.

The free and open internet is largely a creation of American innovators and the light-touch framework that allowed them to work freely without the impositions of nanny-state bureaucrats. Now is the time to recommit to this American system and to defend it from regulatory adventurism in foreign jurisdictions.

Sincerely,

David Williams
President