



**THE FOREIGN CENSORSHIP THREAT:
HOW THE EUROPEAN UNION'S DIGITAL SERVICES ACT COMPELS GLOBAL
CENSORSHIP AND INFRINGES ON AMERICAN FREE SPEECH**

Interim Staff Report of the
Committee on the Judiciary
of the
U.S. House of Representatives



July 25, 2025

EXECUTIVE SUMMARY

The Committee on the Judiciary is investigating how and to what extent foreign laws, regulations, and judicial orders compel, coerce, or influence companies to censor speech in the United States.¹ As part of this oversight, the Committee has issued document subpoenas to nine technology companies, requiring them to turn over communications with foreign censors around the globe.² Documents obtained pursuant to these subpoenas highlight how the European Union (EU) uses a law called the Digital Services Act (DSA) as a censorship tool. The EU claims that the DSA applies only to Europe and that it targets only harmful or illegal content.³ Both of those claims are inaccurate. Nonpublic documents reveal that European regulators use the DSA: (1) to target core political speech that is neither harmful nor illegal; and (2) to pressure platforms, primarily American social media companies, to change their *global* content moderation policies in response to European demands.⁴ Put simply, the DSA infringes on American online speech.

The DSA is the EU's comprehensive digital censorship law.⁵ Passed in 2022, it requires the world's largest online platforms, such as TikTok, X, YouTube, Facebook, and Instagram, to identify and "mitigat[e]" "systemic risks" on their sites, including "misleading or deceptive content" and "disinformation," "any actual or foreseeable negative effects on civil discourse and electoral processes," "hate speech," and "information which is *not* illegal."⁶ To "mitigat[e]" against the risk of "disinformation," "hate speech," and other speech requires a platform to censor user content.⁷ Governments, including the EU, weaponize the terms "disinformation" and "hate speech" to censor their political opponents and criticism from their constituents, including "memes" and other forms of satire.⁸

¹ See, e.g., Press Release, H. Comm. on the Judiciary, *Chairman Jordan Subpoenas Big Tech for Information on Foreign Censorship of American Speech* (Feb. 26, 2025), <https://judiciary.house.gov/media/press-releases/chairman-jordan-subpoenas-big-tech-information-foreign-censorship-american>; Pieter Haeck, *US Presses Brussels for Answers Over EU Social Media Law*, POLITICO (Jan. 31, 2025).

² Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Timothy Cook, CEO, Apple (Feb. 26, 2025) (attaching subpoena); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Andy Jassy, President and CEO, Amazon (Feb. 26, 2025) (attaching subpoena); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Satya Nadella, CEO, Microsoft (Feb. 26, 2025) (attaching subpoena); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Christopher Pavlovski, Chairman and CEO, Rumble (Feb. 26, 2025) (attaching subpoena); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Sundar Pichai, CEO, Alphabet (Feb. 26, 2025) (attaching subpoena); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Custodian of Records, TikTok (Feb. 26, 2025) (attaching subpoena); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Ms. Linda Yaccarino, CEO, X (Feb. 26, 2025) (attaching subpoena); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Mark Zuckerberg, CEO, Meta (Feb. 26, 2025) (attaching subpoena); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Steve Huffman, CEO & President, Reddit (Apr. 17, 2025) (attaching subpoena).

³ See, e.g., Letter from Ms. Henna Virkkunen, Exec. Vice-President for Tech Sovereignty, Security, and Democracy, European Comm'n, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Feb. 18, 2025), Ex. 21.

⁴ See *infra* Section III (The DSA Requires Big Tech Platforms to Change Their Global Content Moderation Policies and Censor Americans), Section IV (European Regulators Are Targeting Core Political Speech and Forcing Global Censorship).

⁵ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) (hereinafter "Digital Services Act").

⁶ See *id.* at recitals 80–84, arts. 34–35 (emphasis added).

⁷ See *id.*

⁸ See *infra* Section IV (European Regulators Are Targeting Core Political Speech and Forcing Global Censorship).

The DSA incentivizes social media companies to comply with the EU’s censorship demands because the penalties for failing to do so are massive.⁹ Platforms deemed noncompliant with the DSA can be fined up to six percent of their global revenue.¹⁰ If “extraordinary circumstances lead to a serious threat to public security or public health in the Union,” regulators are even empowered to temporarily shut down platforms within the EU.¹¹ The EU has explicitly stated that the DSA penalties are intended to be “dissuasive” to companies that would otherwise permit free speech and open political debate on their platforms.¹²

The Committee has been investigating how the DSA imposes global censorship requirements and chills American free speech. This inquiry began in August 2024, when then-EU Commissioner for Internal Market Thierry Breton threatened to weaponize the DSA and target X with regulatory retaliation for broadcasting a live interview with President Trump in the United States.¹³ Following the Committee’s engagement with Breton, he resigned under pressure from EU President Ursula von der Leyen.¹⁴ Despite a new slate of EU Commissioners, the European censorship threat remains. Breton’s successor, Executive Vice-President for Tech Sovereignty, Security, and Democracy Henna Virkkunen, remains strongly supportive of the DSA’s censorship provisions and continues to enforce them against American companies.¹⁵

How the DSA creates a global censorship regime.

The text of the DSA includes a wide array of provisions incentivizing tech companies to censor speech, including speech outside of Europe. Article 21 mandates that platforms allow certified third-party arbitrators to resolve content moderation disputes.¹⁶ 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.¹⁷

⁹ See Digital Services Act, *supra* note 5, at art. 52.

¹⁰ *Id.*

¹¹ *Id.* at art. 36; *Civil society gets its confirmation from EU Commissioner: no internet shutdowns under DSA*, ACCESS NOW (Aug. 2, 2023), <https://www.accessnow.org/press-release/commissioner-breton-responds-dsa/> (former EU Commissioner Breton confirming that the DSA authorizes “temporary shutdowns”).

¹² Digital Services Act, *supra* note 5, at art. 52.

¹³ See Letter from Mr. Thierry Breton, Comm’r for Internal Market, European Comm’n, to Mr. Elon Musk, Owner, X Corp. (Aug. 12, 2024), Ex. 16.

¹⁴ See Lorne Cook, *A French Member of the European Commission Resigns and Criticizes President von der Leyen*, AP (Sept. 16, 2024); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Thierry Breton, Comm’r for Internal Market, European Comm’n (Sept. 10, 2024), Ex. 19; Letter from Thierry Breton, Comm’r for Internal Market, European Comm’n, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 21, 2024), Ex. 18; Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Thierry Breton, Comm’r for Internal Market, European Comm’n (Aug. 15, 2024), Ex. 17.

¹⁵ See, e.g., Pieter Haeck, *EU Won’t Negotiate on Tech Rule Books in Trump Trade Talks, Brussels Says*, POLITICO (July 1, 2025) (“The European Union’s rules on content moderation, digital competition and artificial intelligence are not up for negotiation with the U.S., the European Commission’s tech chief Henna Virkkunen says.”); Adam Satariano, *E.U. Prepares Major Penalties Against Elon Musk’s X*, N.Y. TIMES (last updated Apr. 9, 2025) (reporting that the EU is preparing to fine X an amount that “could ultimately surpass \$1 billion . . . as regulators seek to make an example of X to deter other companies from violating the law, the Digital Services Act.”); *Confirmation Hearing of Henna Virkkunen, Executive Vice-President-Designate of the European Commission*, Jointly by Comm. on Industry, Res., and Energy & Comm. on the Internal Mkt. and Consumer Protection of the European Parliament, Report Hearing, at 13-16 (Nov. 12, 2024).

¹⁶ Digital Services Act, *supra* note 5, at art. 21.

¹⁷ See *infra* Section III.A.1.

In addition, platforms bear the cost when they lose at arbitration, incentivizing them to censor content that has been flagged as potentially violative before arbitration begins.¹⁸

Similarly, DSA Article 22 requires that platforms give priority to censorship requests from government-approved third parties known as “trusted flaggers.”¹⁹ 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.²⁰

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.”²¹ Platforms are specifically warned that this systemic risk may include “information which is *not* illegal.”²² Then, under the DSA, platforms must mitigate these risks, meaning they ultimately must remove content that European regulators deem “misleading,” “deceptive,” or “hate[ful].”²³

Finally, the DSA imposes additional censorship obligations on companies through allegedly voluntary “codes of conduct” on hate speech and disinformation.²⁴ The DSA encourages platforms to work with pro-censorship pseudoscientists and think tanks to draw up best practices for mitigating common systemic risks, known as “codes of conduct.”²⁵ Compliance with these codes effectively serves as a safe harbor against DSA enforcement, meaning that platforms have tremendous incentives to implement them.²⁶ The additional censorship requirements imposed by these codes are substantial. Under the code of conduct relating to disinformation, for example, platforms must agree to use third-party fact-checking on their platforms.²⁷

Moreover, despite their name, the codes of conduct are not “voluntary.” Nonpublic emails between the European Commission (“the Commission”) and technology companies show that Commission regulators repeatedly and deliberately reached out to pressure reluctant

¹⁸ Digital Services Act, *supra* note 5, at art. 21.

¹⁹ *Id.* at art. 22.

²⁰ *See infra* Section III.A.2.

²¹ Digital Services Act, *supra* note 5, at recitals 80–84, art. 34.

²² *Id.* at recital 84 (emphasis added).

²³ *See id.* at recitals 80, 84, 86; *see also infra* Section IV.A.

²⁴ Digital Services Act, *supra* note 5, at art. 45.

²⁵ *Id.*

²⁶ *See, e.g., The Code of Conduct on Disinformation*, EUROPEAN COMM’N, (Feb. 13, 2025), <https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation> (hereinafter “Code of Conduct on Disinformation”) (stating that the code is a “relevant benchmark of DSA compliance.”); *The Code of Conduct on Countering Illegal Hate Speech Online* +, EUROPEAN COMM’N, (Jan. 20, 2025), <https://digital-strategy.ec.europa.eu/en/library/code-conduct-countering-illegal-hate-speech-online> (hereinafter “Code of Conduct on Hate Speech”) (stating that adherence to the code can be considered as appropriate risk mitigation under DSA Article 35).

²⁷ *The Code of Conduct on Disinformation*, EUROPEAN COMM’N, (Feb. 13, 2025), <https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation> (stating that the code is a “relevant benchmark of DSA compliance.”).

platforms to join the ostensibly “voluntary” codes.²⁸ When pressure did not work, the Commission retaliated against the platforms. As one example, X left the Code of Conduct on Disinformation in May 2023 because of the code’s obligations related to third-party fact-checkers, which X generally does not use.²⁹ In October 2023, less than two months after the DSA’s obligations became legally binding, Commission regulators opened an investigation into X’s use of Community Notes instead of fact-checkers.³⁰ Now, the Commission reportedly plans to fine X more than \$1 billion for non-compliance with the DSA.³¹

The DSA is being used to censor political speech, including humor and satire.

On paper, the DSA is bad. In practice, it is even worse. 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. The censorship is largely one-sided, almost uniformly targeting political conservatives. Worse, European regulators expect platforms to deliver on DSA censorship demands by changing their *global* content moderation policies, meaning that European censorship may affect what Americans can say and see online.

On May 7, 2025, the Commission, the enforcer of the DSA, hosted the “DSA Multi-Stakeholder Workshop.”³² Unlike several contemporaneous workshops about the Digital Markets Act (DMA), the EU’s competition legislation, the Commission refused to let the public watch the DSA workshop and specifically told platforms to not share information about it.³³

Communicating about the workshop

The workshop has been publicly announced by the European Commission and will be accompanied by public communication outputs, in full respect of the Chatham House Rule referred to above. These may include, but are not limited to, an event summary or similar communication assets, as well as social media posts. When communicating about the event to external audiences,

- Do not: describe the exercise scenarios / name participants / attribute comments to participants without permission
- You can: interview and use quotes from individuals if given explicit permission / talk about the overall topic of the workshop and the tracks / take photos of the event on the condition that persons in the photos agree and no confidential information (such as the scenario) is shown in the photo

Commission told platforms not to publicly share details about the May 2025 workshop.

²⁸ See, e.g., Emails between European Comm’n and American Platform (Oct. 8, 2021), Ex. 11.

²⁹ Francesca Gillett, *Twitter Pulls out of Voluntary EU Disinformation Code*, BBC (May 27, 2023).

³⁰ Press Release, European Comm’n, *The Commission sends request for information to X under the Digital Services Act* (Oct. 11, 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4953.

³¹ Satariano, *supra* note 15.

³² DSA Multi-Stakeholder Workshop Agenda (May 7, 2025), Ex. 1.

³³ *Id.*; cf. Press Release, European Comm’n, *Commission organises DMA compliance workshops with Alphabet, Amazon, Apple, ByteDance, Meta, and Microsoft* (May 13, 2025), https://digital-markets-act.ec.europa.eu/commission-organises-dma-compliance-workshops-alphabet-amazon-apple-bytedance-meta-and-microsoft-2025-05-13_en.

Documents obtained by the Committee under subpoena reveal what Commission officials told platforms privately and offer critical insights into the DSA censorship process.³⁴ Exercises from the Commission’s May 2025 workshop show the true definitions of key terms in the DSA and Commission regulators’ censorship expectations of social media platforms.³⁵ For example, the Commission’s workshop labeled a hypothetical social media post stating “we need to take back our country”—a common, anodyne political statement—as “illegal hate speech” that platforms are required to censor under the DSA.³⁶

TRACK: 1 – DISSEMINATION OF ILLEGAL CONTENT – AFTERNOON SESSION	
Scenario	5 min
Amira is a 16-year-old Muslim girl who has a history of feeling self-conscious about her identity and has struggled with online harassment in the past. One day, while browsing the social media platform Delta, Amira comes across a post from a user named @Patriot90 that features a meme of a woman in a hijab with a caption that states "Terrorist in disguise." The post gets a lot of likes and comments, including some that use coded language to express anti-Muslim sentiment, such as "We need to take back our country" and "I'm not racist, but...". Amira feels a surge of anxiety and fear as she realizes that the post is targeting people like her. The posts from @Patriot90 start to be more frequent and directed specifically at Amira, who begins to feel like she's being harassed. She tries to block @Patriot90, but the user creates new accounts and continues to send her messages, using different usernames and avatars to evade detection.	
Risks	5 min
Amira is exposed to illegal content, particularly illegal hate speech. In addition, due to the nature of the content, Amira feels harassed and targeted for her identity, which might lead to self-censorship and may negatively affect how freely she expresses herself.	
Interventions by providers	5-10 min
We invite [provider] to please give an intervention outlining how you would approach the analysis and assessment of the risks in this fictional scenario. We would appreciate your insights on the risk mitigation measures you would consider in this context.	

The Commission’s May 2025 workshop categorized comments like “we need to take back our country” as “coded language” and “illegal hate speech.”

The documents also reveal that humor and satire are top censorship targets under the DSA. For example, the Commission’s workshop asked platforms how they could use “content moderation processes” to “address . . . memes that may be used to spread hate speech or discriminatory ideologies.”³⁷ Content targeted by the EU—core political speech, humor, parody, and satire—is protected under any reasonable free speech legal regime, including the First

³⁴ DSA Multi-Stakeholder Workshop Agenda (May 7, 2025), Ex. 1.

³⁵ *Id.*

³⁶ *Id.*

³⁷ *Id.* (emphasis added); *Cf.* STAFF OF THE H. COMM. ON THE JUDICIARY AND THE SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE CENSORSHIP-INDUSTRIAL COMPLEX: HOW TOP BIDEN WHITE HOUSE OFFICIALS COERCED BIG TECH TO CENSOR AMERICANS, TRUE INFORMATION, AND CRITICS OF THE BIDEN ADMINISTRATION (Comm. Print May 1, 2024).

Amendment to the U.S. Constitution. Yet in Europe, and potentially around the world, social media platforms must censor political opinions, humor, and satire that runs afoul of the EU's censorship regime.

The DSA is forcing companies to change their *global* content moderation policies.

The nonpublic materials from the May 2025 workshop make clear that Commission regulators expect platforms to change their worldwide terms and conditions to comply with DSA obligations. During the session, Commission regulators asked platforms how they “should . . . review and update terms and conditions based on the [DSA] risks they identified on their platform” and “take [DSA-identified] potential risks into account” when “designing new (or updating) content moderation policies/guidelines.”³⁸

These questions are intended to support the preparation of participants for the event. During the event, the moderators will facilitate the discussion and invite participants to react to one another's interventions rather than strictly following the questions below.

- How could platform Delta analyse and assess how the design, features and functioning of their platform influence the dissemination of illegal hate speech?
- How could platform Delta analyse and assess how its terms and conditions influence the dissemination of illegal content on their platform?
- What processes should platform Delta have in place to review and update terms and conditions based on the risks they identified on their platform?
- In the risk analysis and assessment, how can platform Delta consider specific regional or linguistic aspects, for example those specific to Member States?
- How can content moderation processes address the use of coded language or memes that may be used to spread hate speech or discriminatory ideologies?
- How could platform Delta analyse and assess the risk of false positives and false negatives when moderating illegal content (both for automated and human reviewed content)?
- What methods could platform Delta use to evaluate user adoption and engagement with the reporting tools for illegal hate speech, especially among minors?
- How could platform Delta cooperate with trusted flaggers, other providers, or civil society organizations to detect and prevent the spread of illegal content?
- How can in-platform awareness-raising measures be designed and implemented to effectively prevent the spread of illegal hate speech? What methods could platform Delta use to evaluate the effectiveness of tools such as “Kindness Reminders” to curb the dissemination of illegal hate speech?
- How can platform Delta analyse and assess how manipulated imagery, such as deepfakes or AI-generated content, are used to spread hate speech or discriminatory ideologies?

The May 2025 workshop's discussion questions demonstrate that Commission regulators expect platforms to work with pro-censorship think tanks, target humor, and change their global terms of service.

Major social media platforms generally have one set of terms and conditions that apply worldwide. This means that the DSA requires platforms to change content moderation policies that apply in the United States, and apply EU-mandated standards to content posted by American

³⁸ DSA Multi-Stakeholder Workshop Agenda (May 7, 2025), Ex. 1.

citizens.³⁹ The threat to American speech is clear: European regulators define political speech, humor, and other First Amendment-protected content as “disinformation” and “hate speech,” and then require platforms to change their global content moderation policies to censor it.⁴⁰

Internal company readouts of the May 2025 workshop also highlight that civil society organizations (CSOs) empowered under the DSA are left-wing and pro-censorship. During the session, CSOs pushed platforms to define terms like “hate speech” and “disinformation” broadly, stating that “content moderation efforts must go beyond illegality” and “address harmful content and disinformation.”⁴¹ Several CSOs expressed a belief that “labelling is not enough when it comes to hate,” even when allegedly hateful content is “not illegal,” and one CSO even said “content moderation efforts should . . . lead to removal of *everything* that can be considered as hateful and harmful.”⁴² Some organizations are also serving as out-of-court arbitrators or trusted flaggers.

----- Forwarded message -----
From: [REDACTED]
Date: Wed, Jul 2, 2025 at 1:02 PM
Subject: DSA Risk Assessment Roundtable - readout
To: [REDACTED]

As for the CSOs that were present at the meeting, I checked and I can't find any list, but I can point at some I remember meeting there:

- ISD Institute for Strategic Dialogue - panel on disinformation, quite aggressive and critical against platforms not working with fact checkers.
- Representative of EDMO (network of EU fact checkers and researchers): the most aggressive (see in the readout)
- Access Now: claiming platforms' content moderation efforts should go beyond illegal content and lead to removal of everything that can be considered as hateful and harmful.

One NGO even argued that “everything that can be considered as hateful and harmful” should be removed.

EU member state takedowns show the target is conservative speech.

Censorship requests from individual EU member states paint the same picture as the Commission’s workshop. Under the DSA, national-level authorities have the power to issue fast-track censorship orders to platforms.⁴³ Like the Commission, individual EU member states target speech on political issues. Three instructive examples come from Poland, France, and Germany.

³⁹ See, e.g., *Community Standards*, META, <https://transparency.meta.com/policies/community-standards/> (last visited July 21, 2025) (“Our Community Standards apply to everyone, all around the world, and to all types of content, including AI-generated content.”); *YouTube Community Guidelines Enforcement*, GOOGLE, <https://transparencyreport.google.com/youtube-policy/removals?hl=en> (last visited July 21, 2025) (“YouTube’s Community Guidelines are enforced consistently across the globe, regardless of where the content is uploaded.”).

⁴⁰ See Digital Services Act, *supra* note 5, recitals 80, 84, 86.

⁴¹ DSA Multi-Stakeholder Workshop Internal Read-Out, Ex. 2.

⁴² *Id.* (emphasis added).

⁴³ Digital Services Act, *supra* note 5, at art. 9.

In 2024, Poland’s National Research Institute (NASK) flagged for TikTok a post that simply stated that “electric cars are neither ecological nor an economical solution”—core political speech on an important topic of public policy.⁴⁴

creation_date	risk_id	intake_portal	country_name	reporting_team_agency
11/25/24 14:15			Poland	NASK
details				
It has been suggested that electric cars are neither an ecological nor an economical solution.				
clean_case_summary				
Investigation Details EMEA Nov 25: Reported content: Sticker translation: Electric cars are the future? #business #mission #economy #politics #intelligence #europeanunion #poland #ukraine #greendeal #ecology IM assessment: unable to confirm violation, no ASR available. Looped in PL PES for review EMEA Nov 26: No violation according to PES Enforcement Action Details N/A - No violation				
reported_entity	final_action_taken	other_info		
https://www.tiktok.com/@biznesmisja/video/7440473235617107222?_r=1&_t=8revglmrPeQ	No Action			

Internal TikTok documents detail Poland’s request to censor speech about electric cars.

Regulators in Europe also are quick to censor criticism of Europe’s disastrous mass migration policy. For example, in 2023, the French National Police directed X to remove a post from a U.S.-based account that satirically noted that a terrorist attack perpetrated by a Syrian refugee may have been caused by permissive French immigration and citizenship policies.⁴⁵



French regulators targeted a U.S.-based account’s tweet about immigration policy.

⁴⁴ Submission by Polish National Research Institute to TikTok (Nov. 25, 2024), Ex. 8.

⁴⁵ Submission by French National Police to X (June 11, 2023), Ex. 9.

Similarly, in December 2024, German authorities classified a tweet calling for the deportation of criminal aliens as “incitement to hatred,” “incitement to violence,” and an “attack on human dignity,” implying that X needed to remove the post.⁴⁶

Description:

The user refers to a Focus online article from 8 August in which a Syrian family is reported to have committed 110 criminal offences and the father blames the youth welfare office.

The user comments: 'Deport the whole lot of them'

Legal Evaluation:

According to our evaluation here, this could be relevant under criminal law pursuant to Section 130 sentence 1 StGB, German Criminal Code (incitement to hatred, incitement to violence and arbitrary measures or attacks on human dignity). Here, hatred is incited against a national group (Syrians) and violence and arbitrary measures are called for.

According to Section 4 sentence (1) No. 3 JMStV, Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and Telemedia, this could be an unauthorised offer with the same content: The author incites hatred against parts of the population or against a national group or a group defined by its ethnicity, and attacks the human dignity of those belonging to this group by insulting, maliciously denigrating or defaming parts of the population or this group.

Ludwigshafen, 09.12.2024

pg

German authorities targeted a tweet calling for deportation of criminal aliens.

* * *

Taken together, the evidence is clear: the Digital Services Act requires the world’s largest social media platforms to engage in censorship of core political discourse in Europe, the United States, and around the world. The Commission classifies important conversations on key political topics as “hate speech” that must be censored under the DSA. Then, it warns platforms that they must change their global content moderation policies to comply with the DSA’s mandates. The mounting evidence is clear that the Digital Services Act infringes upon Americans’ First Amendment right to engage in free and open debate in the modern town square.

This report marks another step in the Committee’s comprehensive investigation of foreign threats to U.S. speech. The Committee continues to receive documents responsive to our subpoenas from around the world, and we will continue to conduct oversight to inform legislative reforms that protect the First Amendment rights of American citizens.⁴⁷

⁴⁶ Submission by German authorities to X (Dec. 9, 2024), Ex. 10.

⁴⁷ See, e.g., H.R. 1071, No Censors on our Shores Act, 119th Cong. (2025).

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
TABLE OF CONTENTS	10
I. THE DIGITAL SERVICES ACT – A GLOBAL CENSORSHIP LAW.....	11
II. THE COMMITTEE IS INVESTIGATING EUROPEAN THREATS TO AMERICAN FREE SPEECH. ..	16
III. THE DSA REQUIRES BIG TECH PLATFORMS TO CHANGE THEIR GLOBAL CONTENT	
MODERATION POLICIES AND CENSOR AMERICANS.....	18
A. The DSA’s mandates lead to increased censorship.	19
1. DSA Article 21: Out-of-court dispute settlement	20
2. Article 22: Trusted flaggers	20
3. Articles 34 and 35: VLOP mandates	22
4. Article 45: So-called “voluntary” codes of conduct	23
B. The DSA’s penalties lead to increased censorship.	25
IV. EUROPEAN REGULATORS ARE TARGETING CORE POLITICAL SPEECH AND FORCING	
GLOBAL CENSORSHIP.	25
A. European Commission regulators classify political debate, satire, and memes as “hate	
speech.”	26
B. European Commission Regulators Expect Platforms to Change their Global Content	
Moderation Policies.	30
C. The European Commission is trying to hide its censorship efforts.	32
D. Empowered by the DSA, European national regulators target core political speech for	
censorship.	33
1. Censorship Target #1: Questioning the effectiveness of electric vehicles	33
2. Censorship Target #2: Satire and questioning Europe’s mass migration policies	34
3. National Regulators Can Issue Global Takedowns.	36
V. CONCLUSION.....	37
APPENDIX	38

I. THE DIGITAL SERVICES ACT – A GLOBAL CENSORSHIP LAW.

The Digital Services Act is the European Union’s comprehensive online censorship law.⁴⁸ Passed on October 19, 2022, the DSA imposes significant legal obligations on the world’s largest social media companies, categorized by the DSA as “Very Large Online Platforms” (VLOPs).⁴⁹ At its core, the DSA requires VLOPs to identify and mitigate “systemic risks” existing on their platforms, including “misleading or deceptive content, including disinformation[,]” “any actual or foreseeable negative effects on civil discourse and electoral processes[,]” and “hate speech[,]” including “information which is *not* illegal.”⁵⁰ Platforms that do not censor enough content to please European regulators face fines up to six percent of their *global* revenue, and if “extraordinary circumstances lead to a serious threat to public security or public health in the Union,” regulators are even empowered to temporarily shut down platforms within the EU.⁵¹

The DSA’s roots date back to at least 2016. Like many efforts to root out so-called “misinformation,” the idea for a large-scale European digital censorship law was inspired by narratives of pervasive Russian interference in the 2016 U.S. presidential election and the 2017 French presidential election. On this theory, Russian social media activities swung the 2016 U.S. election from Hillary Clinton to Donald Trump and nearly defeated Emmanuel Macron in France in 2017.⁵² These sensationalist allegations are unmoored from fact: academic studies have found that Russia’s social media activities ahead of the 2016 U.S. election had little impact on the outcome,⁵³ and Macron is now in his second term as President of France. Yet they have had significant effects on research and policymaking, fueling a global cottage industry of pseudoscientists and pro-censorship think tanks while spurring lawmakers around the world to consider—and ultimately enact—draconian social media regulations that infringe on the right to speak freely online in the digital town square.

The EU’s first response to these allegations was a Commission Recommendation—a non-binding resolution approved by the EU’s executive arm—in March 2018.⁵⁴ This Recommendation urged platforms to have transparent content moderation policies and reporting mechanisms, to use automated content moderation mechanisms, and to cooperate with member states to remove “illegal content.”⁵⁵ In April 2018, the Commission informed the European Parliament of a new plan to combat online disinformation, including plans to develop industry-

⁴⁸ See Digital Services Act, *supra* note 5.

⁴⁹ *Id.*

⁵⁰ *Id.* at recitals 80–84, art. 34 (emphasis added).

⁵¹ *Id.* at arts. 36, 52; *Civil society gets its confirmation from EU Commissioner: no internet shutdowns under DSA*, ACCESS NOW (Aug. 2, 2023), <https://www.accessnow.org/press-release/commissioner-breton-responds-dsa/> (former EU Commissioner Breton confirming that the DSA authorizes “temporary shutdowns”).

⁵² See, e.g., Angelique Chrisafis, *France Says Russian Hackers Behind Attack on Macron’s 2017 Presidential Campaign*, THE GUARDIAN (Apr. 29, 2025); Phillip Rucker, *‘I Would be Your President’: Clinton Blames Russia, FBI Chief for 2016 Election Loss*, WASH. POST (May 3, 2017).

⁵³ See, e.g., Gregory Eady et al., *Exposure to the Russian Internet Research Agency Foreign Influence Campaign on Twitter in the 2016 US Election and Its Relationship to Attitudes and Voting Behavior*, 14 NATURE COMM’NS 62 (2023); Tim Starks, *Russian Trolls on Twitter had Little Influence on 2016 Voters*, WASH. POST (Jan. 9, 2023).

⁵⁴ Commission Recommendation (EU) 2018/334 of 1 March 2018 on Measures to Effectively Tackle Illegal Content Online, 2018 O.J. (L 63/50).

⁵⁵ *Id.*

wide best practices for countering alleged disinformation.⁵⁶ These initial steps, which largely lacked enforcement mechanisms and relied on voluntary compliance, were criticized as insufficient by the growing chorus of misinformation pseudoscientists and the increasingly pro-censorship political left.⁵⁷ Heeding these calls, the EU began to contemplate a comprehensive digital censorship law, which would ultimately become the DSA.

In June 2020, the Commission requested comment from tech platforms and other stakeholders on the development of legislation to address so-called “disinformation” online.⁵⁸ Then, in December 2020, the Commission released full legislative proposals for a Digital Services Act and a sister competition bill, the Digital Markets Act.⁵⁹ This first draft of the DSA included the core risk assessment and mitigation framework that remains the law’s centerpiece, and explicitly contemplated that the industry-wide best practices drafted in 2018—formally known as the Code of Conduct on Disinformation—would be incorporated under the DSA.⁶⁰

After nearly a year of negotiations, the Council of the European Union—a legislative body with one representative from each EU member state—agreed to an amended DSA in November 2021.⁶¹ Most notably, the Council granted “exclusive enforcement power” to the Commission, though it did preserve national regulators’ ability to issue content takedown orders directly to platforms.⁶² In January 2022, the European Parliament—the EU’s primary legislative body, directly elected by citizens of each member state—made further amendments, primarily related to algorithmic manipulation and advertising.⁶³ In April 2022, the Council and the Parliament made a “provisional agreement” to approve the DSA.⁶⁴ Even the *New York Times* noted that the primary purpose of the bill was to “force . . . internet services to combat misinformation” and “address[] online speech” in a way that would be “off limits in the United States” because of the First Amendment.⁶⁵

⁵⁶ Communication from the Comm’n to the European Parliament, the Council, the European Econ. & Social Comm. and the Comm. of the Regions, *Tackling Online Disinformation: A European Approach*, COM(2018) 236 final (Apr. 26, 2018).

⁵⁷ See, e.g., Ethan Shattock, *Self-Regulation 2.0? A Critical Reflection of the European Fight Against Disinformation*, HARV. MISINFORMATION REV. (May 31, 2021) (arguing that new legislation should “end the era of haphazard self-regulation that has characterized the EU response to disinformation.”).

⁵⁸ Natasha Lomas, *Europe Asks for Views on Platform Governance and Competition Tools*, TECHCRUNCH (June 2, 2020).

⁵⁹ See, e.g., Mark Scott et al., *Europe Rewrites Rulebook for Digital Age*, POLITICO (Dec. 15, 2020).

⁶⁰ Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC, COM (2020) 825 final (Dec. 15, 2020).

⁶¹ Press Release, Council of the European Union, *What is illegal offline should be illegal online: Council agrees position on the Digital Services Act* (Nov. 25, 2021), <https://www.consilium.europa.eu/en/press/press-releases/2021/11/25/what-is-illegal-offline-should-be-illegal-online-council-agrees-on-position-on-the-digital-services-act/>.

⁶² *Id.*

⁶³ Amendments Adopted by the European Parliament on Jan. 20, 2022, on the Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC, COM(2020) 825 final (2020/0361(COD)).

⁶⁴ Press Release, Council of the European Union, *Digital Services Act: Council and European Parliament provisional agreement for making the internet a safer space for European citizens* (Apr. 23, 2022), <https://www.consilium.europa.eu/en/press/press-releases/2022/04/23/digital-services-act-council-and-european-parliament-reach-deal-on-a-safer-online-space/>.

⁶⁵ Adam Satariano, *E.U. Takes Aim at Social Media’s Harms With Landmark New Law*, N.Y. TIMES (Apr. 22, 2022).

The European Parliament formally passed the DSA on July 5, 2022, by a vote of 539 to 54.⁶⁶ Opposition to the bill was concentrated on the political right, though several right-of-center parties voted for the bill.⁶⁷ The Council of the European Union approved the DSA on October 4, 2022,⁶⁸ and the Presidents of the Council and Parliament signed it into law on October 19, 2022.⁶⁹

Despite the DSA's complex and vague set of edicts, enforcement began rapidly.⁷⁰ The Commission designated seventeen entities as VLOPs, which are subject to the most stringent regulations, on April 25, 2023.⁷¹ These entities—thirteen of which were American⁷²—had just four months to come into compliance with the DSA's requirements, and the Commission began to enforce them almost immediately thereafter.⁷³ The Commission initiated DSA compliance investigations into Facebook, Instagram, X, and TikTok in October 2023, less than two months after the law's requirements for VLOPs went into effect.⁷⁴ In December 2023, the Commission opened formal proceedings against X for choosing to use Community Notes rather than allow third-party fact-checkers to censor content, and for moving to a subscription-based model for blue checkmarks.⁷⁵ In April 2024, the Commission initiated formal proceedings against Meta for the “non-availability of an effective third-party real-time civic discourse and election-monitoring tool”—essentially, for failure to adequately censor election-related content.⁷⁶ Both proceedings remain open, and public reporting indicates that the Commission could fine X over \$1 billion for alleged non-compliance with the DSA, though the Commission has denied the reporting.⁷⁷ The

⁶⁶ Press Release, European Parliament, *Digital Services: landmark rules adopted for a safer, open online environment* (July 5, 2022), <https://www.europarl.europa.eu/news/en/press-room/20220701IPR34364/digital-services-landmark-rules-adopted-for-a-safer-open-online-environment>.

⁶⁷ *Digital Services Act*, HOWTHEYVOTE.EU (July 5, 2022), <https://howtheyvote.eu/votes/146649>.

⁶⁸ Press Release, Council of the European Union, *DSA: Council gives final approval to the protection of users' rights online* (Oct. 4, 2022), <https://www.consilium.europa.eu/en/press/press-releases/2022/10/04/dsa-council-gives-final-approval-to-the-protection-of-users-rights-online/>.

⁶⁹ IMCO Committee Press (@EP_SingleMarket), X (Oct. 19, 2022, 10:58 AM), https://x.com/EP_SingleMarket/status/1582748151030874114.

⁷⁰ The Commission opened its first DSA investigations less than a year after the law was passed. See Press Release, European Comm'n, *The Commission sends request for information to X under the Digital Services Act* (Oct. 11, 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4953. This stands in contrast to other recent EU digital regulations. For example, the General Data Protection Regulation (GDPR) came into effect two full years after its passage. See *Legal Framework of EU Data Protection*, EUROPEAN COMM'N, https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en (last visited July 21, 2025).

⁷¹ *The Enforcement Framework Under the Digital Services Act*, EUROPEAN COMM'N, <https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement> (last updated Feb. 12, 2025).

⁷² *Supervision of the Designated Very Large Online Platforms and Search Engines Under DSA*, EUROPEAN COMM'N, <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses> (last updated July 14, 2025).

⁷³ *The Enforcement Framework Under the Digital Services Act*, EUROPEAN COMM'N, <https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement> (last updated Feb. 12, 2025).

⁷⁴ *Id.*

⁷⁵ Press Release, European Comm'n, *Commission opens formal proceedings against X under the Digital Services Act* (Dec. 17, 2023); https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709.

⁷⁶ Press Release, European Comm'n, *Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act* (Apr. 30, 2024); <https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-facebook-and-instagram-under-digital-services-act>.

⁷⁷ Satariano, *supra* note 15.

Commission also initiated DSA proceedings against Meta, TikTok, AliExpress, and Temu for violations related to safeguards for minors and consumer protection in 2024.⁷⁸

These enforcement actions are changing content moderation worldwide—and that was the goal of the EU. From the very beginning, the DSA was intended to have global effects. At the time of its passage, then-European Minister for Industry and Trade Jozef Sikela hoped that the DSA would become “the ‘gold standard’ for other regulators in the world.”⁷⁹ Shortly after the DSA’s requirements for VLOPs came into effect, *The New York Times* reported that “[EU] officials and experts hope” that the DSA’s “effects could extend far beyond Europe, *changing company policies in the United States and elsewhere*.”⁸⁰

TECHNOLOGY**The New York Times**

E.U. Law Sets the Stage for a Clash Over Disinformation

The law, aimed at forcing social media giants to adopt new policies to curb harmful content, is expected to face blowback from Elon Musk, who owns X.

The law, the Digital Services Act, is intended to force social media giants to adopt new policies and practices to address accusations that they routinely host — and, through their algorithms, popularize — corrosive content. **If the measure is successful, as officials and experts hope, its effects could extend far beyond Europe, changing company policies in the United States and elsewhere.**

⁷⁸ Press Release, European Comm’n, *Commission opens formal proceedings against Temu under the Digital Services Act* (Oct. 30, 2024), https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5622; Press Release, European Comm’n, *Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram* (May 15, 2024), https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2664; Press Release, European Comm’n, *Commission opens formal proceedings against AliExpress under the Digital Services Act* (Mar. 13, 2024), https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1485; Press Release, European Comm’n, *Commission opens formal proceedings against TikTok under the Digital Services Act* (Feb. 18, 2024), https://ec.europa.eu/commission/presscorner/detail/en/ip_24_926.

⁷⁹ Press Release, Council of the European Union, *DSA: Council gives final approval to the protection of users’ rights online* (Oct. 4, 2022), <https://www.consilium.europa.eu/en/press/press-releases/2022/10/04/dsa-council-gives-final-approval-to-the-protection-of-users-rights-online/>.

⁸⁰ Steven Lee Myers, *E.U. Law Sets the Stage for a Clash Over Disinformation*, N.Y. TIMES (Sept. 27, 2023) (emphasis added).

Academics have argued that the DSA would likely affect speech in the United States, writing that the DSA will “incentivize the platforms to remove large swaths of content” and “alter their globally applicable terms of service and content moderation guidelines in response to the DSA’s mandates in ways that will be speech-restrictive worldwide.”⁸¹ Sadly, some on the American left have cheered on this phenomenon. Former Secretary of State Hillary Clinton “urge[d]” the European Parliament to “push the Digital Services Act across the finish line[.]”⁸² while other prominent American progressives have lamented the First Amendment’s protection of free speech.⁸³

The DSA is also specifically anti-American, designed to saddle American tech companies with burdensome regulations while leaving European companies free to innovate. Under the DSA, platforms with more than 45 million monthly users are designated as VLOPs and subject to the strictest regulations.⁸⁴ This arbitrary threshold appears to have been drawn to sweep in major American companies while carving out Europe’s top tech companies. Outside of pornography websites, the only European VLOP is Booking.com, which has faced virtually no scrutiny from Commission regulators.⁸⁵ For other European tech companies, the Commission has invented workarounds to exempt them from the VLOP designation. The Commission, however, has allowed Spotify, for the purpose of counting EU users, to split its products into music and podcasts.⁸⁶ Spotify claims that its music streaming service does not involve user-generated content and therefore can be severed from its podcasting service which qualifies as user-generated content.⁸⁷ By severing its products, Spotify counts only its podcasting users, which it claims are fewer than 45 million in the EU, and therefore, escapes VLOP designation and the DSA’s most onerous regulations.⁸⁸ Observers have noted that there are “flaw[s] in the methodology” of the EU’s VLOP designation process and that there is “a clear discrepancy” between Spotify’s actual European user numbers and the numbers the Commission accepts.⁸⁹

The DSA is not the only tool in this campaign to kneecap American tech, either. The Digital Markets Act (DMA), the DSA’s sister legislation, imposes strict requirements on the design of internet services for large platforms known as “gatekeepers.”⁹⁰ The DMA’s qualitative

⁸¹ Dawn Carla Nunziato, *The Digital Services Act and the Brussels Effect on Platform Content Moderation*, 24 CHIC. J. INT. LAW 115, 122 (2023).

⁸² Hillary Clinton (@HillaryClinton), X (Apr. 21, 2022, 5:02 PM), <https://x.com/HillaryClinton/status/1517247388716613634>.

⁸³ See, e.g., Jonathan Turley, *Opinion: Vance is Right. Harris and Walz are a Threat to Americans’ Free Speech*, USA TODAY (Oct. 3, 2024) (noting Gov. Tim Walz’s comment that “there’s no guarantee to free speech on misinformation or hate speech”); Lindsay Kornick, *John Kerry Calls the First Amendment a ‘Major Block’ to Stopping ‘Disinformation’*, FOX NEWS (Sept. 29, 2024) (“John Kerry called the First Amendment a ‘major block’ to combating misinformation and fighting climate change.”).

⁸⁴ Digital Services Act, *supra* note 5, at art. 33.

⁸⁵ *Supervision of the Designated Very Large Online Platforms and Search Engines Under DSA*, EUROPEAN COMM’N, <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses> (last updated July 14, 2025).

⁸⁶ Martin Husovec, *The DSA’s Scope Briefly Explained*, SSRN (July 4, 2023).

⁸⁷ *Id.*

⁸⁸ *Id.*; Digital Services Act, *supra* note 5, at art. 33.

⁸⁹ *The EU must hold VLOPs accountable*, ACCESS NOW (last updated Jan. 4, 2024).

⁹⁰ *The Digital Markets Act: Ensuring Fair and Open Digital Markets*, EUROPEAN COMM’N, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en (last visited July 21, 2025).

standards for designating gatekeepers are even more ripe for abuse—and indeed, the Commission has once again used them to target American companies. Like the DSA, the only European “gatekeeper” is Booking.com, which has not been targeted by European regulators despite reports that it is out of compliance with the DMA.⁹¹ Conversely, Apple and Meta were recently fined a collective 700 million euros for alleged non-compliance with the DMA.⁹²

The DSA is premised on a faulty reading of history. It is built on a belief that government cannot trust citizens to freely decide what is true or to handle online content that might offend them. The anti-speech, Big Brother law is shaping online discourse in Europe and around the world. The EU’s comprehensive digital regulation scheme targets American companies and infringes on American speech online.

II. THE COMMITTEE IS INVESTIGATING EUROPEAN THREATS TO AMERICAN FREE SPEECH.

The Committee has been investigating European threats to American free speech for nearly a year. This effort began in August 2024, when then-EU Commissioner for Internal Market Thierry Breton threatened X with regulatory retaliation under the DSA for hosting a live interview with President Trump in the United States.⁹³ Just a few hours before President Trump’s scheduled interview, Breton wrote a letter to Elon Musk, X’s owner, warning that “spillovers” of U.S. speech into the EU could spur the Commission to adopt “interim” retaliatory “measures” against X under the DSA.⁹⁴ Breton warned that he would be “extremely vigilant to any evidence” that President Trump’s interview spilled over into the EU and informed Musk that the Commission “[would] not hesitate to make full use of [its] toolbox” to silence this core American political speech.⁹⁵

Three days later, the Committee wrote to Breton, demanding that he stop “any attempt to intimidate individuals or entities engaged in political speech in the United States” or “otherwise interfere in the American democratic process.”⁹⁶ Breton responded to the Committee with a letter in which he downplayed his threatening statements and obfuscated the censorship provisions of the DSA.⁹⁷ He stated, wrongly, that “[t]he DSA does not regulate content” and inaccurately said that “[w]e would send a similar reminder to any of the DSA regulated entities . . . under similar circumstances”—despite no evidence that the Commission had ever sent a similar letter to a different platform ahead of live-streamed political events in the United States.⁹⁸

⁹¹ *Booking.com Fails to Comply with Digital Markets Act, HOTREC Reports*, HOTEL NEWS RESOURCE (Nov. 14, 2024).

⁹² Press Release, European Comm’n, *Commission finds Apple and Meta in breach of the Digital Markets Act* (Apr. 22, 2025), https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085.

⁹³ Letter from Mr. Thierry Breton, Comm’r for Internal Market, European Comm’n, to Mr. Elon Musk, Owner, X Corp. (Aug. 12, 2024), Ex. 16.

⁹⁴ *Id.*

⁹⁵ *Id.*

⁹⁶ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Thierry Breton, Comm’r for Internal Market, European Comm’n (Aug. 15, 2024), Ex. 17.

⁹⁷ Letter from Thierry Breton, Comm’r for Internal Market, European Comm’n, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 21, 2024), Ex. 18.

⁹⁸ *Id.*

The Committee responded to Breton with a second letter, noting the inaccuracies in his letter and accepting his offer for a briefing on the DSA.⁹⁹ Shortly after this second letter, Breton resigned under pressure from EU President Ursula von der Leyen.¹⁰⁰ Committee staff received a briefing from the EU Delegation to the U.S. on October 2, 2024, in which EU staff repeated Breton's claims.¹⁰¹

After Breton's initial letter to Elon Musk, the Committee also wrote to the State Department to request a briefing on the Biden-Harris Administration's efforts to stem the tide of European censorship and "protect against foreign attempts to shut down constitutionally protected speech in the United States."¹⁰² On September 5, 2024, the Biden-Harris State Department informed Committee staff that it did not intend to publicly condemn Breton's threats or take any other action in response to this attack on a U.S. company and American speech.¹⁰³

The Breton incident was simply the first flashpoint in a growing clash over free speech. Despite Breton's resignation, the EU retained the ability to weaponize the DSA as Breton threatened.¹⁰⁴ Breton's successor, Henna Virkkunen, serves as the Executive Vice-President for Tech Sovereignty, Security, and Democracy, and continues to actively enforce the DSA against American companies and supports its censorship provisions.¹⁰⁵ Shortly after Virkkunen's confirmation, the Committee wrote a letter "to express our serious concerns with how the DSA's censorship provisions affect free speech in the United States."¹⁰⁶ Like her predecessor, Virkkunen responded by making the misleading claim that "the DSA does not regulate speech."¹⁰⁷ The Committee's engagement with Virkkunen and Commission regulators continues.

To better understand the foreign censorship demands on American social media companies, on February 26, 2025, the Committee issued document subpoenas to eight online platforms, compelling Alphabet, Amazon, Apple, Meta, Microsoft, Rumble, TikTok, and X to

⁹⁹ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Thierry Breton, Comm'r for Internal Market, European Comm'n (Sept. 10, 2024), Ex. 19.

¹⁰⁰ Lorne Cook, *A French Member of the European Commission Resigns and Criticizes President von der Leyen*, AP (Sept. 16, 2024).

¹⁰¹ EU briefing with Committee Staff (Oct. 2, 2024).

¹⁰² Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Uzra Zeya, Under Sec'y for Civilian Security, Democracy, & Human Rights, and Hon. Eileen Donahoe, Special Envoy & Coordinator for Digital Freedom, Dep't of State (Aug. 15, 2024).

¹⁰³ State Department briefing with Committee staff (Sept. 5, 2024).

¹⁰⁴ See, e.g., House Judiciary GOP (@JudiciaryGOP), X (Nov. 1, 2024, 10:06 AM), <https://x.com/JudiciaryGOP/status/1852351403030687924>.

¹⁰⁵ See, e.g., Pieter Haeck, *EU Won't Negotiate on Tech Rule Books in Trump Trade Talks, Brussels Says*, POLITICO (July 1, 2025) ("The European Union's rules on content moderation, digital competition and artificial intelligence are not up for negotiation with the U.S., the European Commission's tech chief Henna Virkkunen says."); Satariano, *supra* note 15 (reporting that the EU is preparing fines to X that "could ultimately surpass \$1 billion . . . as regulators seek to make an example of X to deter other companies from violating the law, the Digital Services Act."); *Confirmation Hearing of Henna Virkkunen, Executive Vice-President-Designate of the European Commission*, Jointly by Comm. on Industry, Res., and Energy & Comm. on the Internal Mkt. and Consumer Protection of the European Parliament, Report Hearing, at 13-16 (Nov. 12, 2024).

¹⁰⁶ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Ms. Henna Virkkunen, Exec. Vice-President for Tech Sovereignty, Security, and Democracy, European Comm'n (Jan. 31, 2025), Ex. 20.

¹⁰⁷ Letter from Ms. Henna Virkkunen, Exec. Vice-President for Tech Sovereignty, Security, and Democracy, European Comm'n, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Feb. 18, 2025), Ex. 21.

produce their communications with foreign censors—including the European Union and its member states.¹⁰⁸ At the time of these subpoenas, the Committee also wrote to foreign leaders, warning them that the Committee would begin to receive content moderation-related communications from their governments and encouraging them to support fundamental free speech principles.¹⁰⁹ On April 17, the Committee issued an additional document subpoena to Reddit.¹¹⁰ Under these subpoenas, the tech companies are compelled to turn over content moderation-related communications with regulators from the EU and its member states as they happen—and dating as far back as 2020.¹¹¹ Because the subpoenas are continuing in nature, the Committee continues to receive productions, including of censorship pressure and takedown requests that have occurred since the issuance of the subpoenas. This interim staff report is drawn from the nonpublic documents produced to the Committee under subpoena.

III. THE DSA REQUIRES BIG TECH PLATFORMS TO CHANGE THEIR GLOBAL CONTENT MODERATION POLICIES AND CENSOR AMERICANS.

The EU claims that the DSA’s objective is to merely ensure a “safe, predictable, and trusted online environment” by addressing illegal content and societal risks associated with the spreading of disinformation.¹¹² Although ostensibly well-intentioned, the DSA leads to censorship, namely censorship of conservative viewpoints. First, the DSA defines illegal content “broadly.”¹¹³ Additionally, the DSA contains provisions not just focusing on illegal content, but on content contributing to identified categories of systemic risks, which are also broadly defined.¹¹⁴ For example, one systemic risk category is “actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, as well as public security.”¹¹⁵ This

¹⁰⁸ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Timothy Cook, CEO, Apple (Feb. 26, 2025) (attaching subpoena); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Andy Jassy, President and CEO, Amazon (Feb. 26, 2025) (attaching subpoena); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Satya Nadella, CEO, Microsoft (Feb. 26, 2025) (attaching subpoena); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Christopher Pavlovski, Chairman and CEO, Rumble (Feb. 26, 2025) (attaching subpoena); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Sundar Pichai, CEO, Alphabet (Feb. 26, 2025) (attaching subpoena); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Custodian of Records, TikTok (Feb. 26, 2025) (attaching subpoena); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Ms. Linda Yaccarino, CEO, X (Feb. 26, 2025) (attaching subpoena); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Mark Zuckerberg, CEO, Meta (Feb. 26, 2025) (attaching subpoena).

¹⁰⁹ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Ms. Ursula von der Leyen, President, European Comm’n (Feb. 27, 2025), Ex. 22; Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to His Excellency Luiz Inácio Lula da Silva, President of Brazil (Feb. 27, 2025); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to The Rt. Hon. Sir Keir Starmer, Prime Minister of the United Kingdom (Feb. 27, 2025).

¹¹⁰ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Steve Huffman, CEO & President, Reddit (Apr. 17, 2025) (attaching subpoena).

¹¹¹ *Id.*

¹¹² Digital Services Act, *supra* note 5, at recital 9.

¹¹³ *Id.* at recital 12 (noting “to achieve the objective of ensuring a safe, predictable, and trustworthy online environment, for the purpose of this Regulation. . . the concept of ‘illegal content’ should be defined broadly”).

¹¹⁴ *Id.* at recitals 80–84.

¹¹⁵ *Id.* at recital 83. The other systemic risk categories are illegal content dissemination; “the actual or foreseeable impact of the service on the exercise of fundamental rights; and “negative effects on the protection of public health, minors, and serious negative consequences to a person’s physical and mental well-being, or on gender-based violence.” See Digital Services Act, *supra* note 5, at recitals 80–82 and 84.

vague definition means that the DSA does not just govern content widely considered to be harmful, like child sexual abuse material, but also content that EU bureaucrats believe negatively affects elections or civic discourse.

To achieve its censorship goal, the DSA requires all online platforms to allow individuals and entities to notify them about content the individuals and entities consider illegal.¹¹⁶ Platforms must also provide a complaint handling system allowing individuals and entities to submit complaints if they disagree with platform decisions on how to handle content and allow individuals and entities to take their dispute to out-of-court settlement bodies for ultimate resolution.¹¹⁷ Further, the DSA mandates platforms swiftly resolve “trusted flagger” notifications, which are notifications submitted to platforms from entities EU officials identify as having, among other requirements, expertise in detecting illegal content.¹¹⁸ If these requirements were not burdensome enough, the DSA imposes additional mandates on VLOPs, or platforms with a monthly average of more than 45 million EU users.¹¹⁹ Specifically, VLOPs must identify and mitigate systemic risks originating from their services.¹²⁰

The DSA’s mandates are a significant burden on platforms. The Committee has received testimony from tech company executives about the costs of complying with the DSA. In a recent transcribed interview with the Committee, YouTube’s Global Head of Trust and Safety testified that it took numerous teams within YouTube a “very significant amount of effort to comply with” the DSA.¹²¹

To ensure compliance with its mandates, the DSA permits the European Commission to impose fees up to six percent of a platform’s worldwide revenue.¹²² The DSA also empowers regulators to restrict access to a platform under certain circumstances.¹²³ When combined, the DSA’s extensive mandates and severe penalties lead platforms to err on the side of more censorship—removing not only illegal content, but any content European regulators could find problematic. This censorship affects not only European users, but users worldwide, including Americans.

A. The DSA’s mandates lead to increased censorship.

The DSA’s burdensome mandates cause tech companies and social media platforms to censor content. These mandates include those related to out-of-court dispute settlement, trusted flaggers, VLOPs, and codes of conduct.

¹¹⁶ Digital Services Act, *supra* note 5, at art. 16.

¹¹⁷ *Id.* at arts. 20–21.

¹¹⁸ *Id.* at art. 22. (explaining trusted flagger status is achieved if entities also demonstrate they are independent from online platforms and “carry out their activities for the purposes of submitting notices diligently, accurately, and objectively.”).

¹¹⁹ Digital Services Act, *supra* note 5, at art. 33.

¹²⁰ *Id.* at arts. 34–35.

¹²¹ Transcribed Interview of YouTube’s Vice President, Global Head of Trust and Safety, H. Comm. on the Judiciary (June 12, 2025) (on file with the Comm.).

¹²² Digital Services Act, *supra* note 5, at arts. 52, 73.

¹²³ *Id.* at arts. 51, 82.

1. DSA Article 21: Out-of-court dispute settlement

The DSA mandates that platforms allow the use of out-of-court dispute settlements to resolve disagreements between platforms and individuals and entities that notify platforms of alleged objectionable content. This mandate effectively encourages platforms to censor content.

Under the DSA, platforms must allow individuals and entities to use certified out-of-court dispute settlement bodies to resolve disputes involving platform decisions on flagged content.¹²⁴ Platform decisions eligible for out-of-court dispute settlement include decisions to not remove flagged content and decisions not to suspend a user for content they post.¹²⁵ For example, Article 21 allows individuals who notified a platform of content they thought was hate speech to dispute a platform's decision not to remove the content.¹²⁶ If the settlement body finds against the platform, the platform is solely responsible for fees that the body charges to hear the dispute.¹²⁷

Only settlement bodies certified by European regulators are allowed to hear these disputes.¹²⁸ Although settlement bodies must be financially independent from platforms, they need not be financially independent from EU regulators.¹²⁹ As such, the settlement bodies can be entirely funded by EU member governments, which calls into question their ability to make unbiased determinations. Due to their lack of independence, it follows that settlement bodies will generally make determinations based on what EU regulators want. Because platforms are fully responsible for costs associated with the settlement if platforms lose disputes, there is a large incentive for platforms to adhere to the censorship demands to avoid paying settlement costs. In this way, the DSA incentivizes platforms to censor content that is flagged as problematic by individuals or entities.

2. Article 22: Trusted flaggers

Like the DSA's out-of-court settlement provision, the DSA's provision on trusted flaggers also encourages censorship. Under the DSA, trusted flaggers may notify platforms about hate speech, disinformation, or other content EU regulators find problematic.¹³⁰ Unlike requests from regular individuals and entities, the law requires platforms to prioritize notifications from trusted flaggers and make decisions "without undue delay."¹³¹ Additionally, trusted flaggers must publish reports to EU regulators outlining the notifications given to platforms and the actions platforms took in response.¹³² This requirement means that European regulators can see

¹²⁴ Digital Services Act, *supra* note 5, at art. 21.

¹²⁵ *See id.* at arts. 20–21. The full list of platform decisions subject to out-of-court settlement are decisions whether or not to: (1) "remove or disable access to or restrict visibility" of the flagged information; (2) "suspend or terminate the provision of the service, in whole or in part" to certain users; (3) "suspend or terminate" a user's account; and (4) "suspend, terminate or otherwise restrict the ability [of a user] to monetize information." Digital Services Act *supra* note 5, at art. 20.

¹²⁶ *See id.* at arts. 20–21.

¹²⁷ *Id.* at art. 21.

¹²⁸ *Id.*

¹²⁹ *Id.*

¹³⁰ *Id.* at art. 22.

¹³¹ Digital Services Act, *supra* note 5, at art. 22.

¹³² *Id.*

whether platforms agree with trusted flaggers to censor content or whether platforms decide to keep content available.

Importantly, trusted flaggers need to be independent only from platforms.¹³³ They otherwise do not need to be independent or non-partial. Trusted flaggers can be entities incentivized to get platforms to censor content. For example, the Finnish designated trusted flagger Somis Enterprises Oy, a flagger focused on illegal speech, is a company marketing itself as a specialist in preventing bullying and harassment.¹³⁴ The more content the company can get removed from platforms, the greater it can market itself to potential customers as being a successful business, which can lead to increased profits.

Trusted flaggers can also have relationships with European regulators. For example, the French designated trusted flagger e-Enfance, which focuses on illegal speech, public security risks, and violence, receives support from the Commission and France's Education Ministry.¹³⁵ Another French designated trusted flagger, Association Point de Contact, also specializing in illegal speech, public security risks, and violence, states it works closely with France's Ministry of Interior.¹³⁶ A subsection of the Ministry, the "Prefecture de Police," responsible for policing, even serves as an observing member to the Association Point de Contact with an "advisory role."¹³⁷

This lack of independence renders meaningless a DSA provision that appears on its face to be favorable to platforms. Under the DSA, if a trusted flagger submits frivolous notifications, European regulators can investigate and suspend the entity's trusted flagger status.¹³⁸ However, if trusted flaggers have relationships with regulators, there is reason to question whether this conflict of interest would result in trusted flaggers not facing any consequences for over-flagging. If trusted flaggers are able to force platforms to investigate trivial notices with little to no consequence, the flaggers could overwhelm platforms with content to be reviewed until platforms change their global content moderation policies.

Even more concerning, trusted flaggers can have current conflicts with the online platforms to which they are charged with sending notifications. For example, the German designated trusted flagger, Hate Aid, which specializes in cyber violence and illegal speech, is currently in litigation with X, a platform subject to DSA regulation, and thus a platform to which

¹³³ *Id.* at art. 22.

¹³⁴ *Company Information*, SOMETURVA, <https://www.someturva.fi/us/> (last visited July 21, 2025).

¹³⁵ *The e-Enfance/3018 Association Fights Against Harassment and Digital Violence Suffered by Young People*, E-ENFANCE 3018, <https://e-enfance.org/#> (last visited July 21, 2025); *The e-Enfance/3018 Association Has Been Supported Since Its Creation by a Network of Trusted Partners*, E-ENFANCE 3018, <https://e-enfance.org/qui-sommes-nous/partenaires/> (last visited July 21, 2025).

¹³⁶ *About Point of Contact*, POINT DE CONTACT.NET, <https://www.pointdecontact.net/a-propos/> (last visited July 21, 2025); *Members of Point of Contact*, POINT DE CONTACT.NET, <https://www.pointdecontact.net/nos-membres/> (last visited July 21, 2025).

¹³⁷ *Members of Point of Contact*, POINT DE CONTACT.NET, <https://www.pointdecontact.net/nos-membres/> (last visited July 21, 2025); *Ministry of the Interior (France)*, FUND IT, <https://fundit.fr/en/institutions/ministry-interior-france> (last visited July 21, 2025).

¹³⁸ See Digital Services Act, *supra* note 5, at art. 22.

Hate Aid can submit notices.¹³⁹ Without independence, trusted flaggers can either advance their own interests and/or be pressured by or work in concert with regulators, to flag content in hopes that platforms censor the content. Because European regulators will know whether platforms censor content flagged by trusted flaggers, platforms are incentivized to agree with trusted flaggers and censor content to avoid conflict with regulators. This is especially true for VLOPs, which have additional mandates under the DSA.

3. Articles 34 and 35: VLOP mandates

In addition to requirements applicable to all platforms, the DSA imposes additional mandates on VLOPs, which further encourage censorship.¹⁴⁰ European regulators attempt to justify these additional mandates by arguing that VLOPs can strongly influence online safety, public discourse, and public opinion.¹⁴¹ However, as described above, evidence suggests VLOP designation and its additional requirements are used to burden non-European technology companies with compliance costs.¹⁴² VLOP designation also appears to be used as an additional means to censor speech.

One VLOP-specific requirement is a mandate to conduct an annual risk assessment analyzing, identifying, and assessing whether any “systemic risks in the [European] Union stemming from the design or functioning of [a platform’s] service and its related systems” are present.¹⁴³ Importantly, as explained above, systemic risks involve more than illegal content.¹⁴⁴ Systemic risks also include actual or foreseeable: (1) “negative effects on civic discourse and electoral processes and public security”; (2) negative effects relating to the protection of public health and negative consequences to a person’s physical and mental well-being; and (3) negative effects for exercising fundamental rights.¹⁴⁵ In fact, the DSA explicitly outlines how VLOPs, when assessing systemic risks, should “focus” on “information which is not illegal” and “pay particular attention” to misleading or deceptive content, including disinformation.¹⁴⁶ The DSA also directs platforms to specifically note in risk assessments where “algorithmic amplification of information”—in other words the reach of content—contributes to systemic risks.¹⁴⁷ This requirement means that the DSA directs companies to not only assess how content produced within the EU contributes to systemic risks, but also how content produced in places like the United States that spreads to the EU contributes to systemic risks. Notably, the DSA fails to clearly define systemic risks, giving regulators discretion as to what exact content contributes to such risks. This ambiguity is likely by design as it puts pressure on VLOPs to be broad when carrying out the next VLOP-specific requirement—risk mitigation.

¹³⁹ See e.g., *For Independent Re-Search: Landmark Case Against X*, HATE AID, <https://hateaid.org/en/for-independent-research-landmark-case-against-x/> (last visited July 21, 2025).

¹⁴⁰ Digital Services Act, *supra* note 5, at arts. 33–35.

¹⁴¹ *Id.* at recital 79.

¹⁴² See *Supervision of the Designated Very Large Online Platforms and Search Engines Under DSA*, EUROPEAN COMM’N, <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses> (last updated July 14, 2025).

¹⁴³ Digital Services Act, *supra* note 5, at art. 34.

¹⁴⁴ See *id.* at recitals 80–84.

¹⁴⁵ *Id.* at art. 34.

¹⁴⁶ *Id.* at recital 84.

¹⁴⁷ *Id.*

Once VLOPs conduct risk assessments, they must develop and implement mitigation measures to reduce identified risks.¹⁴⁸ Mitigation measures include VLOPs adapting their terms and conditions, changing enforcement of terms and conditions, and adapting content moderation policies to more effectively remove content.¹⁴⁹ These mitigation measures are particularly concerning as companies often have only one set of policies they apply globally.¹⁵⁰ Thus, any changes made to policies to comply with DSA-mandated risk mitigation, like increasing the content that is censored, can affect all users, not just those in the EU.¹⁵¹ By requiring VLOPs to mitigate wide-ranging systemic risks, the DSA drives VLOPs towards censorship. Especially when used in conjunction with the DSA’s “codes of conduct”—voluntary standards drafted alongside pro-censorship groups that can be used as benchmarks for compliance—these mitigation measures likely result in more censorship.

4. Article 45: So-called “voluntary” codes of conduct

The DSA’s use of codes of conduct are another tool that European regulators use to incentivize VLOPs to censor content. To ensure proper application of DSA provisions like mandated risk mitigation, the DSA encourages VLOPs to create “voluntary” codes of conduct when the same systemic risks concern several VLOPs.¹⁵² Codes of conduct must take “due account of the needs and interests of all interested parties,” which include European regulators and pro-censorship interest groups.¹⁵³ Thus, final codes of conduct could be significantly more burdensome than what VLOPs would otherwise draft.

The codes are effectively mandatory as they are often used as a benchmark to assess VLOPs’ compliance with the DSA.¹⁵⁴ One example is the Code of Conduct on Countering Illegal Hate Speech Online +, which notes how adherence to the code can be considered as appropriate risk mitigation under DSA Article 35.¹⁵⁵ Under this code, signatories must have terms and conditions prohibiting “illegal” hate speech, allow EU users to report hate speech, and strengthen partnerships with nonprofit or public entities with expertise on hate speech.¹⁵⁶

¹⁴⁸ Digital Services Act, *supra* note 5, at art. 35.

¹⁴⁹ *See id.*

¹⁵⁰ *See, e.g., Community Standards*, META, <https://transparency.meta.com/policies/community-standards/> (last visited July 21, 2025) (“Our Community Standards apply to everyone, all around the world, and to all types of content, including AI-generated content.”); *YouTube Community Guidelines Enforcement*, GOOGLE, <https://transparencyreport.google.com/youtube-policy/removals?hl=en> (last visited July 21, 2025) (“YouTube’s Community Guidelines are enforced consistently across the globe, regardless of where the content is uploaded.”).

¹⁵¹ *See Nunziato, supra* note 81 (“In short, the DSA’s substantive content moderation and notice and take down provisions will likely incentivize the platforms to remove large swaths of content . . . And the platforms will likely alter their globally applicable terms of service and content moderation guidelines in response to the DSA’s mandates in ways that will be speech-restrictive worldwide.”).

¹⁵² Digital Services Act, *supra* note 5, at art. 45.

¹⁵³ *See id.*

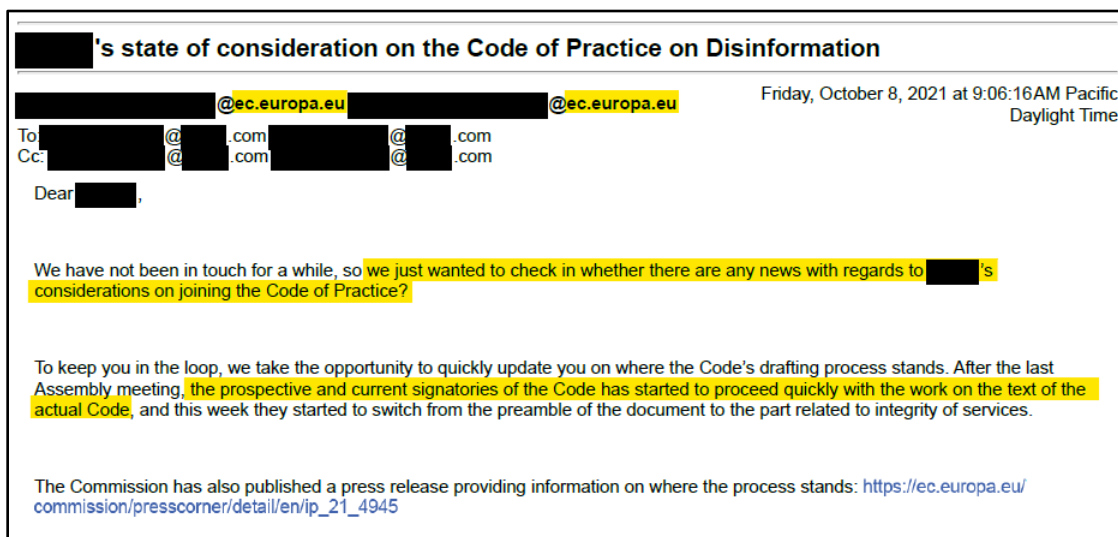
¹⁵⁴ *See The Code of Conduct on Disinformation*, EUROPEAN COMM’N, (Feb. 13, 2025), <https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation>; *Code of Conduct on Hate Speech*, EUROPEAN COMM’N, (Jan. 20, 2025), <https://digital-strategy.ec.europa.eu/en/library/code-conduct-countering-illegal-hate-speech-online>.

¹⁵⁵ *The Code of Conduct on Hate Speech*, EUROPEAN COMM’N, (Jan. 20, 2025), <https://digital-strategy.ec.europa.eu/en/library/code-conduct-countering-illegal-hate-speech-online>.

¹⁵⁶ *Id.* (noting the signatories include “Facebook, Instagram, LinkedIn, Snapchat, X, and YouTube.”).

Another example is the Code of Conduct on Disinformation.¹⁵⁷ Like the Code of Conduct on Countering Illegal Hate Speech Online +, the disinformation code is a “relevant benchmark of DSA compliance.”¹⁵⁸ Disinformation Code signatories commit, in part, to strengthening misinformation and disinformation policies and adopting, reinforcing, and implementing policies governing “impermissible manipulative behaviors and practices.”¹⁵⁹ Signatories also commit to raising awareness about disinformation and to “integrate, showcase, or otherwise consistently use” fact-checkers’ work.¹⁶⁰

The structural pressure notwithstanding, documents obtained by the Committee under subpoena show how European regulators pressure platforms to join on to the ostensibly “voluntary” codes of conduct.¹⁶¹ Regulators make clear that only code signatories have a seat at the code of conduct drafting table.¹⁶² Consequently, because codes of conduct are a benchmark of DSA compliance, companies are pressured to join the codes so that they have some say over what the compliance benchmark entails. Most recently, European regulators have been clearer about their intentions when describing similar “voluntary” codes promulgated under the EU AI Act, confirming that compliance with voluntary codes will “reduce [companies’] administrative burden” and give platforms special access to the Commission.¹⁶³



The Commission pressuring a U.S. company to join the Voluntary Code on Disinformation.

Failing to meet the benchmark, by either not joining or withdrawing from a code, has severe consequences. For example, in May 2023, X withdrew from the Code of Conduct on Disinformation because the code mandated platforms use third-party fact checkers, which X did

¹⁵⁷ See *The Code of Conduct on Disinformation*, EUROPEAN COMM’N, (Feb. 13, 2025), <https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation>.

158 *Id.*

¹⁵⁹ *Id.* (noting the signatories include “Facebook, Instagram, LinkedIn . . . [and] YouTube[.]”).

160 *Id.*

¹⁶¹ See Emails between European Comm'n and American Platform (Oct. 8, 2021), Ex. 11; Emails between European Comm'n and American Platform (Sept. 2021), Ex. 12; Emails between European Comm'n and American Platform (Aug. 2021), Ex. 13; Emails between European Comm'n and American Platform (Feb. 2021), Ex. 14.

¹⁶² Emails between European Comm’n and American Platform (Oct. 8, 2021), Ex. 11.

¹⁶³ Ashely Gold, *EU Lays Out AI Act Compliance Rules*, AXIOS PRO (July 14, 2025).

not use.¹⁶⁴ In October 2023, less than two months after the DSA’s obligations became legally binding on X, the Commission opened an investigation into X’s use of Community Notes instead of fact checkers.¹⁶⁵ X now reportedly faces a more than \$1 billion DSA fine.¹⁶⁶

B. The DSA’s penalties lead to increased censorship.

The DSA’s enormous penalties based on global revenue, such as the reported fine against X, strongly discourage platform noncompliance, increasing the likelihood that platforms follow European regulator demands and censor speech.¹⁶⁷ The DSA does not hide its goal of using huge penalties to encourage total compliance—the law outlines how “penalties shall be. . . dissuasive.”¹⁶⁸ As such, the DSA authorizes fines up to six percent of a platform’s global revenue, a sum potentially totaling billions of dollars for some platforms.¹⁶⁹ The potential for such large fines means that platforms risk significant financial loss if EU regulators determine they are noncompliant with DSA mandates. To avoid such an enormous penalty, platforms are likely to ensure strict DSA compliance.

The DSA’s burdensome mandates, which encourage censorship, combined with the DSA’s costly penalties, create an environment in which platforms are strongly incentivized to censor content rather than uphold free speech principles. Even worse, content likely to be censored is not just illegal speech, but any speech that European regulators label as contributing to broad systemic risks. As the structure of the DSA’s mandates and related codes of conduct also encourage platforms to rethink content policies, which platform usually apply globally, European regulators are essentially forcing a new global free speech paradigm. This European censorship regime significantly restricts fundamental principles of free speech, limiting what individuals, including Americans, can say online.

IV. EUROPEAN REGULATORS ARE TARGETING CORE POLITICAL SPEECH AND FORCING GLOBAL CENSORSHIP.

European officials regularly claim that the DSA “does not regulate content,”¹⁷⁰ “does not regulate speech,”¹⁷¹ and is “content-agnostic.”¹⁷² By the terms of the law, these claims are wrong: the DSA requires VLOPs to take “mitigation measures” against alleged “disinformation” and “hate speech,” which are defined in the DSA as types of “content.”¹⁷³ Now, for the first time, documents obtained by the Committee show the type of online content that is targeted by

¹⁶⁴ Gillett, *supra* note 29.

¹⁶⁵ Press Release, European Comm’n, The Commission sends request for information to X under the Digital Services Act (Oct. 11, 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4953.

¹⁶⁶ Adam Satariano, *supra* note 15.

¹⁶⁷ *Id.*

¹⁶⁸ Digital Services Act, *supra* note 5, at art. 52.

¹⁶⁹ *Id.*; see Jillian Deutsch, *Tech Giants Could Face Billions in Fines Under EU’s New Content Rules*, INS. J. (Apr. 25, 2022).

¹⁷⁰ Letter from Thierry Breton, Comm’r for Internal Market, European Comm’n, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 21, 2024), Ex. 18.

¹⁷¹ Letter from Ms. Henna Virkkunen, Exec. Vice-President for Tech Sovereignty, Security, and Democracy, European Comm’n, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Feb. 18, 2025), Ex. 21.

¹⁷² *Id.*

¹⁷³ Digital Services Act, *supra* note 5, at recitals 9, 84, arts. 34–35.

European anti-speech regulators. Pursuant to the Committee’s February 26, 2025, subpoenas, American tech companies have produced information about their interactions with regulators from the Commission and every EU member state. These documents paint a troubling picture: led by the Commission, European regulators are targeting core political speech that is neither illegal nor harmful. The EU and its member states are using the DSA’s censorship tools to silence conservatives on political topics such as immigration and the environment. And this censorship regime directly threatens Americans’ First Amendment rights.

A. European Commission regulators classify political debate, satire, and memes as “hate speech.”

On May 7, 2025, the Commission hosted a “DSA Multi-Stakeholder Workshop on Systemic Risks and Their Mitigation.”¹⁷⁴ This event brought together platforms, NGOs, and regulators to “discuss the assessment and mitigation of specific risks” under the DSA.¹⁷⁵ Major American VLOPs, including Alphabet, Amazon, Apple, Meta, Microsoft, and X, participated in the event, which was shrouded in secrecy until the agenda was produced to the Committee under subpoena.¹⁷⁶ The workshop included eight breakout sessions in which platforms were given fictional online scenarios and pressed on how they would respond to the systemic risks present in each scenario. Metadata from documents produced to the Committee further indicate that these scenarios were drafted by a European bureaucrat responsible for enforcing the DSA within the Commission’s Directorate General for Communications Networks, Content, and Technology (DG-CNECT).¹⁷⁷

Description

Title:

Author:

Subject:

Keywords:

Created: 5/6/2025 1:43:57 PM

Additional Metadata...

DSA workshop exercises were drafted by a European bureaucrat.

These Commission-drafted exercises shine a light on how the Commission defines terms like “hate speech” and “disinformation” in practice, and what content moderation steps it thinks are required under the DSA.¹⁷⁸ The short version: the Commission’s definition of “hate speech”

¹⁷⁴ DSA Multi-Stakeholder Workshop Agenda (May 7, 2025), Ex. 1; *see also* DSA Multi-Stakeholder Workshop Internal Read-Out, Ex. 2; DSA Multi-Stakeholder Workshop Invitations, Ex. 3-4; DSA Multi-Stakeholder Workshop Thank You and Commission Read-Outs, Ex. 5-6.

¹⁷⁵ DSA Multi-Stakeholder Workshop Agenda (May 7, 2025), Ex. 1.

¹⁷⁶ *Id.*

¹⁷⁷ *Id.*

¹⁷⁸ *Id.*

sweeps in large swaths of legitimate political debate, and the Commission expects platforms to alter their global content moderation policies in order to comply with the DSA.

One exercise in particular displays the Commission’s censorship goals. A breakout session during the workshop focused on the “dissemination of illegal content” and provided specific examples of “illegal hate speech” under the DSA.¹⁷⁹ These included a hypothetical post stating “we need to take back our country.”¹⁸⁰ This common political rhetoric has been used across the political spectrum in the United States—by former Vice President Kamala Harris,¹⁸¹ Senator Elizabeth Warren,¹⁸² and President Donald Trump,¹⁸³ for example—to express dissatisfaction with the status quo and promise political change. Yet, in Europe, simply posting the phrase may be illegal—and platforms must censor it to avoid massive fines.

TRACK: 1 – DISSEMINATION OF ILLEGAL CONTENT – AFTERNOON SESSION	
Scenario	5 min
Amira is a 16-year-old Muslim girl who has a history of feeling self-conscious about her identity and has struggled with online harassment in the past. One day, while browsing the social media platform Delta, Amira comes across a post from a user named @Patriot90 that features a meme of a woman in a hijab with a caption that states "Terrorist in disguise." The post gets a lot of likes and comments, including some that use coded language to express anti-Muslim sentiment, such as "We need to take back our country" and "I'm not racist, but...". Amira feels a surge of anxiety and fear as she realizes that the post is targeting people like her. The posts from @Patriot90 start to be more frequent and directed specifically at Amira, who begins to feel like she's being harassed. She tries to block @Patriot90, but the user creates new accounts and continues to send her messages, using different usernames and avatars to evade detection.	
Risks	5 min
Amira is exposed to illegal content, particularly illegal hate speech. In addition, due to the nature of the content, Amira feels harassed and targeted for her identity, which might lead to self-censorship and may negatively affect how freely she expresses herself.	
Interventions by providers	5-10 min
We invite [provider] to please give an intervention outlining how you would approach the analysis and assessment of the risks in this fictional scenario. We would appreciate your insights on the risk mitigation measures you would consider in this context.	

The Commission’s exercise categorized comments like “we need to take back our country” as “coded language” and “illegal hate speech.”

¹⁷⁹ *Id.*

¹⁸⁰ *Id.*

¹⁸¹ Senator Kamala Harris, Speech to the California Democratic State Convention: Taking Our Country Back (May 20, 2017) (“But I’ll tell you how I believe we take our country back. It starts with you. To take our country back, we need to remember that real power does not reside in Washington, D.C.”)

¹⁸² Ricardo Lewis, *Senator Elizabeth Warren Vows to Fight Fard for Working Families*, DAKOTA NEWS NOW (Jan. 5, 2019) (“‘This is a moment when we should dream big, fight hard and take back our country, thank you,’ Senator Warren said.”).

¹⁸³ Soo Rin Kim et al., *Trump Holds ‘Make America Great Again Victory Rally’ on Inauguration Eve*, ABC NEWS (Jan. 19, 2025) (“I’m thrilled to be back with so many friends, supporters, and true American patriots on the eve of taking back our country. That’s what we’re going to do. Take back our country[.]”).

The Commission’s censorship decisions also appear to be informed by narrow-minded stereotypes of conservatives who exercise their right to speak freely on social media. In the same exercise, the primary perpetrator of “hate speech” is a fictional account with the handle @Patriot90.¹⁸⁴ Tellingly, the Commission depicts a “patriot” not as a citizen who is proud of his national heritage and loves his country, but as someone deplorable.¹⁸⁵ This is the only scenario of the eight in which a fake account name was presented, indicating that social media handles indicating a conservative political affiliation or a general love of country are singled out for censorship under the DSA.¹⁸⁶

Moreover, the exercise makes clear that the Commission targets humor and satire for censorship under the DSA. One discussion question asks how platforms can use “content moderation processes” to “address . . . memes that may be used to spread hate speech or discriminatory ideologies,” and another asks how platforms should “analyse and assess . . . AI-generated content.”¹⁸⁷ Satire, parody, and other forms of humor—including memes and AI-generated photos or videos—are important forms of expression that compellingly highlight government excess, overreach, or absurdity. As political cartoonists have proven for centuries, incisive humor can be among the most effective ways to demonstrate that the political class is out of touch or has lost its way.¹⁸⁸ That is perhaps precisely why the Commission targets them.

Key takeaways:

Areas addressed: DSA reporting systems, mitigation measures related to recommender systems, issues with evaluation of terrorist content and illegal hate speech.

- CSOs pointed at difficulties in using DSA reporting mechanisms and the fact that it is even more problematic for regular/non expert users.
- CSOs called for more efforts to reduce the spread of TCO and illegal hate speech through recommender systems.
- CSOs claimed moderation efforts must go beyond illegality and also better address harmful content and disinformation aimed at dehumanising or inciting hate.
- Some suggested labelling is not enough when it comes to hate, even if not illegal forms of hate.
- Reflections around how platforms prevent risk of over/under-removal, false positives and false negatives.

Civil society organizations empowered under the DSA argued that platforms need to engage in more censorship of legal speech.

¹⁸⁴ DSA Multi-Stakeholder Workshop Agenda (May 7, 2025), *see* Ex. 1.

¹⁸⁵ *Id.*

¹⁸⁶ *Id.*

¹⁸⁷ *Id.*

¹⁸⁸ *See* VICTOR S. NAVASKY, THE ART OF CONTROVERSY: POLITICAL CARTOONS & THEIR ENDURING POWER (2013).

The workshop materials also reaffirm that platforms are expected to work with pro-censorship pseudoscientists and think tanks to censor content. Under Article 22, platforms must give priority to censorship requests from government-approved third-parties, and the exercise materials state that “the engagement of VLOPs . . . with stakeholders and experts is important for the good functioning of the DSA.”¹⁸⁹ The discussion questions clarify what kind of engagement is expected, asking how platforms can proactively “cooperate with trusted flaggers . . . [and] civil society organizations” (CSOs) to “detect and prevent the spread of illegal content”—which, as explained above, includes core political speech.¹⁹⁰ These CSOs uniformly argue in favor of more censorship, meaning that a platform’s cooperation inevitably results in more speech being silenced.

Indeed, one platform’s internal readout of the workshop noted that CSOs argued that “content moderation efforts must go beyond illegality” and “address harmful content and disinformation.”¹⁹¹ Specifically, the CSOs argued for content removals, with some saying that “labelling is not enough when it comes to hate,” even when allegedly hateful content is “not illegal.”¹⁹² In particular, the Commission-funded European Digital Media Observatory (EDMO) complained that X’s “[Community Notes] don’t work.”¹⁹³ One NGO called Access Now went so far as to argue that “content moderation efforts should . . . lead to removal of *everything* that can be considered as hateful and harmful.”¹⁹⁴

----- Forwarded message -----
From: [REDACTED]
Date: Wed, Jul 2, 2025 at 1:02 PM
Subject: DSA Risk Assessment Roundtable - readout
To: [REDACTED]

As for the CSOs that were present at the meeting, I checked and I can’t find any list, but I can point at some I remember meeting there:

- ISD Institute for Strategic Dialogue - panel on disinformation, quite aggressive and critical against platforms not working with fact checkers.
- Representative of EDMO (network of EU fact checkers and researchers): the most aggressive (see in the readout)
- Access Now: claiming platforms’ content moderation efforts should go beyond illegal content and lead to removal of everything that can be considered as hateful and harmful.

One NGO even argued that “everything that can be considered as hateful and harmful” should be removed.

¹⁸⁹ See *infra* Section III.a.2; DSA Multi-Stakeholder Workshop Agenda (May 7, 2025), Ex. 1.

¹⁹⁰ DSA Multi-Stakeholder Workshop Agenda (May 7, 2025), Ex. 1.

¹⁹¹ DSA Multi-Stakeholder Workshop Internal Read-Out, Ex. 2.

¹⁹² *Id.*

¹⁹³ *Id.*

¹⁹⁴ *Id.* (emphasis added).

B. European Commission Regulators Expect Platforms to Change their Global Content Moderation Policies.

Perhaps most importantly, the May 2025 exercise indicates that the Commission expects platforms to change their global terms of service in order to comply with the DSA—meaning that the DSA effectively creates a global censorship standard. Discussion questions posed by the Commission asks how platforms “should . . . review and update terms and conditions based on the [DSA] risks they identified on their platform” and “take [DSA-identified] potential risks into account” when “designing new (or updating) content moderation policies/guidelines.”¹⁹⁵

These questions are intended to support the preparation of participants for the event. During the event, the moderators will facilitate the discussion and invite participants to react to one another's interventions rather than strictly following the questions below.

- How could platform Delta analyse and assess how the design, features and functioning of their platform influence the dissemination of illegal hate speech?
- How could platform Delta analyse and assess how its terms and conditions influence the dissemination of illegal content on their platform?
- What processes should platform Delta have in place to review and update terms and conditions based on the risks they identified on their platform?
- In the risk analysis and assessment, how can platform Delta consider specific regional or linguistic aspects, for example those specific to Member States?
- How can content moderation processes address the use of coded language or memes that may be used to spread hate speech or discriminatory ideologies?
- How could platform Delta analyse and assess the risk of false positives and false negatives when moderating illegal content (both for automated and human reviewed content)?
- What methods could platform Delta use to evaluate user adoption and engagement with the reporting tools for illegal hate speech, especially among minors?
- How could platform Delta cooperate with trusted flaggers, other providers, or civil society organizations to detect and prevent the spread of illegal content?
- How can in-platform awareness-raising measures be designed and implemented to effectively prevent the spread of illegal hate speech? What methods could platform Delta use to evaluate the effectiveness of tools such as “Kindness Reminders” to curb the dissemination of illegal hate speech?
- How can platform Delta analyse and assess how manipulated imagery, such as deepfakes or AI-generated content, are used to spread hate speech or discriminatory ideologies?

The workshop's discussion questions demonstrate that Commission regulators expect platforms to work with pro-censorship think tanks, target humor, and change their global terms of service.

Platforms generally maintain one set of terms and conditions worldwide, meaning that any DSA-mandated changes to content moderation policies are likely to affect speech around the world.¹⁹⁶ Notably, the Commission's use of the word “should” indicates that Commission

¹⁹⁵ *Id.*

¹⁹⁶ See, e.g., *Community Standards*, META, <https://transparency.meta.com/policies/community-standards/> (last visited July 21, 2025) (“Our Community Standards apply to everyone, all around the world, and to all types of content, including AI-generated content.”); *YouTube Community Guidelines Enforcement*, GOOGLE, <https://transparencyreport.google.com/youtube-policy/removals?hl=en> (last visited July 21, 2025) (“YouTube's Community Guidelines are enforced consistently across the globe, regardless of where the content is uploaded.”).

regulators expect platforms to change these global policies to comply with the DSA. If platforms fail to change their terms of service and censor enough content to please European regulators, they can face massive fines under DSA Article 52.¹⁹⁷

The Commission classifies conventional political discourse, including humor, as “hate speech” that must be censored under the DSA. Then, it warns platforms that they must change their terms of service to ensure that this political speech is censored. In practice, the DSA requires social media platforms to censor political speech around the world—including in the United States—because the reach of technology and social media is global.

It is impractical and likely harmful to users’ privacy for large tech companies to try to maintain a separate set of terms and conditions unique to Europe. For example, in order to have geographically distinct content moderation policies, platforms would have to heavily rely on technologies which are invasive and easily circumvented—most likely geo-blocking.¹⁹⁸ For geo-blocking to work, platforms have to collect user information like location and Wi-Fi data.¹⁹⁹ Once collected, some data would have to be stored, which creates the risk of data breaches revealing location and network data for users around the world.²⁰⁰ In addition to these privacy concerns, it is also costly for platforms to stand up, develop, and maintain multiple trust and safety teams to implement and continually maintain separate content moderation policies and the geo-blocking systems.

Further, geo-blocking is ineffective: users can bypass geo-blocking efforts by using virtual private networks (VPNs), which change users’ virtual location by connecting to servers in different countries.²⁰¹ VPNs would allow users to bypass additional content restrictions enacted for one jurisdiction, but not another. Geo-blocking’s ineffectiveness, due in part to VPNs, is one reason regulators in Australia and Brazil have explicitly ordered *global* content removals or threatened to fine users who use VPNs to access geo-blocked content.²⁰²

Finally, even if geo-blocking were an effective solution, and even if platforms could practically implement differing policies based on location, European regulators would still not be satisfied. The DSA, from the beginning, was designed to have effects “in the United States.”²⁰³ To the extent any ambiguity remained once the DSA was enacted, European regulators quickly made it explicit that the DSA was intended to have global effects: most notably, then-EU Commissioner for Internal Market Thierry Breton publicly warned that “spillovers” of U.S.

¹⁹⁷ Digital Services Act, *supra* note 5, at art. 52.

¹⁹⁸ See *Geo-IP Blocking: A Double-Edged Sword for Network Firewall Security*, HOSTOMIZE, <https://hostomize.com/blog/geo-ip/> (last visited July 21, 2025); Aušra Korkuzaitė, *Best VPN for Geo-Blocking in 2025*, CYBERNEWS (last updated July 4, 2025).

¹⁹⁹ See *Geo-IP Blocking: A Double-Edged Sword for Network Firewall Security*, HOSTOMIZE, <https://hostomize.com/blog/geo-ip/> (last visited July 21, 2025).

²⁰⁰ See *id.*

²⁰¹ Aušra Korkuzaitė, *Best VPN for Geo-Blocking in 2025*, CYBERNEWS (last updated July 4, 2025).

²⁰² See e.g., Chad De Guzman, ‘Arrogant Billionaire’: Elon Musk Feuds with Australian PM Over Content Takedown Orders, TIME (Apr. 23, 2024); Fact Check: Brazilians Can Be Fined for Using VPN to Access X, REUTERS (Sept. 6, 2024) (last updated Sept. 9, 2024).

²⁰³ Myers, *supra* note 80.

speech into the EU could be a potential violation of the DSA.²⁰⁴ Quite simply, although the DSA is a law drafted in Europe by Europeans, the DSA intentionally imposes substantial compliance obligations on American tech companies and advances the Europeans’ paternalistic restrictions on online speech globally. In this way, the DSA directly infringes on Americans’ right to speak freely in the modern town square of social media.

C. The European Commission is trying to hide its censorship efforts.

Naturally, the Commission wants to hide its censorship aims—so it instructed workshop participants not to publicly “describe the exercise scenarios” used during the DSA workshop.²⁰⁵ This runs in direct opposition to the DSA’s purported “transparency” principles,²⁰⁶ and is a break in practice from the Commission’s enforcement activities for the Digital Markets Act (DMA), a companion law to the DSA dealing with competition. While DMA “compliance workshop[s]” are open to the public and recorded, the May 2025 DSA workshop was shrouded in secrecy.²⁰⁷ Not only is the EU trying to censor speech around the world—but it is also trying to hide it.

Communicating about the workshop

The workshop has been publicly announced by the European Commission and will be accompanied by public communication outputs, in full respect of the Chatham House Rule referred to above. These may include, but are not limited to, an event summary or similar communication assets, as well as social media posts. When communicating about the event to external audiences,

- Do not: describe the exercise scenarios / name participants / attribute comments to participants without permission
- You can: interview and use quotes from individuals if given explicit permission / talk about the overall topic of the workshop and the tracks / take photos of the event on the condition that persons in the photos agree and no confidential information (such as the scenario) is shown in the photo

Commission regulators told platforms not to publicly share details about the workshop.

²⁰⁴ Letter from Mr. Thierry Breton, Comm’r for Internal Market, European Comm’n, to Mr. Elon Musk, Owner, X Corp. (Aug. 12, 2024), Ex. 16.

²⁰⁵ DSA Multi-Stakeholder Workshop Agenda (May 7, 2025), Ex. 1.

²⁰⁶ See Digital Services Act, *supra* note 5, at art. 42.

²⁰⁷ See, e.g., 2025 Amazon DMA Compliance Workshop, EUROPEAN COMM’N (June 23, 2025), https://digital-markets-act.ec.europa.eu/events-poolpage/2025-amazon-dma-compliance-workshop-2025-06-23_en.

D. Empowered by the DSA, European national regulators target core political speech for censorship.

The DSA also grants significant authority to national digital regulators, giving them power to make censorship demands and requiring platforms to quickly respond.²⁰⁸ This provision, too, is causing censorship of political speech. Three examples produced to the Committee under subpoena demonstrate that national-level regulators are using the DSA to target political speech about environmental policy and immigration.

1. Censorship Target #1: Questioning the effectiveness of electric vehicles

The first censorship example comes from Poland, where in November 2024, the National Research Institute (NASK), within the Ministry of Digital Affairs, asked TikTok to remove a post that simply stated that “electric cars are neither ecological nor an economical solution.”²⁰⁹ This statement is core political speech, making a claim about the effectiveness and feasibility of widespread electric car usage. The only possible objection to the post is disagreement with its content—demonstrating that European regulators, far from being “content-agnostic,” weaponize their censorship tools to attack political speech with which they disagree.²¹⁰

creation_date	risk_id	intake_portal	country_name	reporting_team_agency
11/25/24 14:15			Poland	NASK
details				
It has been suggested that electric cars are neither an ecological nor an economical solution.				
clean_case_summary				
Investigation Details EMEA Nov 25: Reported content: Sticker translation: Electric cars are the future? #business #mission #economy #politics #intelligence #europeanunion #poland #ukraine #greenddeal #ecology IM assessment: unable to confirm violation, no ASR available. Looped in PL PES for review EMEA Nov 26: No violation according to PES Enforcement Action Details N/A - No violation				
reported_entity	final_action_taken	other_info		
https://www.tiktok.com/@biznesmisja/video/7440473235617107222?_r=1&t=8revginrPeQ	No Action			

Internal TikTok documents detail Poland’s request to censor speech about electric cars.

²⁰⁸ Digital Services Act, *supra* note 5, at art. 9.

²⁰⁹ Submission by Polish National Research Institute to TikTok (Nov. 25, 2024), Ex. 8.

²¹⁰ Letter from Ms. Henna Virkkunen, Exec. Vice-President for Tech Sovereignty, Security, and Democracy, European Comm’n, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Feb. 18, 2025), Ex. 21.

2. Censorship Target #2: Satire and questioning Europe's mass migration policies

In 2023, French regulators took steps to silence debate about immigration following a brutal attack in which a Syrian refugee stabbed several young children and parents on a playground in the city of Annecy.²¹¹ In the aftermath of the attack, French digital regulators ordered platforms to remove not only videos of the attack, but also post-attack commentary about immigration and refugee policy.

For example, French authorities targeted one an X post from a U.S.-based account satirically noting that the attack may have been caused by permissive French immigration and citizenship policies.²¹² The post is clearly part of ongoing and much larger political debate about the effect of immigration policy on the safety of citizens. Yet, rather than allowing true debate in the marketplace of ideas, French authorities attempted to censor the viewpoint.



French regulators targeted a U.S.-based account's tweet about immigration policy.

²¹¹ See Aurelien Breeden, *Stabbing in France Critically Injures 4 Children, Shocking Country*, N.Y. TIMES (June 8, 2023).

²¹² Submission by French National Police to X (June 11, 2023), Ex. 9.

German censors similarly sought to silence discussion about immigration. In August 2024, a German X user tweeted “deport the whole lot of them” in response to a news article about a family of Syrian aliens that had reportedly “committed 110 criminal offenses” during their time in Germany.²¹³ More than four months later, German authorities classified this call for the deportation of criminal aliens as “incitement to hatred,” “incitement to violence,” and an “attack[] on human dignity,” implying that X needed to remove the post.²¹⁴ Once again, European regulators targeted political speech on a topic of major public debate.

Description:

The user refers to a Focus online article from 8 August in which a Syrian family is reported to have committed 110 criminal offences and the father blames the youth welfare office.

The user comments: ‘Deport the whole lot of them!’

Legal Evaluation:

According to our evaluation here, this could be relevant under criminal law pursuant to Section 130 sentence 1 StGB, German Criminal Code (incitement to hatred, incitement to violence and arbitrary measures or attacks on human dignity). Here, hatred is incited against a national group (Syrians) and violence and arbitrary measures are called for.

According to Section 4 sentence (1) No. 3 JMStV, Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and Telemedia, this could be an unauthorised offer with the same content: The author incites hatred against parts of the population or against a national group or a group defined by its ethnicity, and attacks the human dignity of those belonging to this group by insulting, maliciously denigrating or defaming parts of the population or this group.

Ludwigshafen, 09.12.2024

pg

German authorities targeted a tweet calling for deportation of criminal aliens.

In the Polish and French examples, the platforms refused to censor the flagged speech outside of the requesting country, meaning that in these cases, Americans’ speech rights were not violated. In the German example, the tweet at issue is no longer accessible, although the reason why is unclear. Regardless, these cases illuminate that European censors, both at the Commission and national levels, intend to silence debate on important political, economic, social, and cultural topics. The DSA gives them the tools they need to do so.

²¹³ Submission by German authorities to X (Dec. 9, 2024), Ex. 10.

²¹⁴ *Id.*

3. National Regulators Can Issue Global Takedowns.

Under current EU judicial precedent, these national-level takedowns could become global. In a major 2019 case, the European Court of Justice, Europe’s highest court, ruled that individual EU member states can issue *global* content takedown orders.²¹⁵ In *Eva Glawischnig-Piesczek v. Facebook Ireland Ltd.*, the case centered on core political speech involving a public figure: a Facebook user called the former leader of Austria’s Green Party, Eva Glawischnig-Piesczek, a “lousy traitor,” “corrupt oaf” and member of a “fascist party.”²¹⁶ At the time, experts warned that the decision, which ultimately pre-dated the DSA by only a few years, “foreshadow[ed] future disputes over Europe’s role in setting rules on the internet.”²¹⁷

While explicit global takedown orders by European countries have not been common, increased use of judicial orders targeting posts for worldwide removal could constitute a major threat to U.S. speech.²¹⁸ Moreover, as regulators become increasingly frustrated by the use of VPNs to sidestep their censorship orders, countries, such as Australia, have explicitly ordered global content removals.²¹⁹

On those grounds, the Court (Third Chamber) hereby rules:

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (*‘Directive on electronic commerce’*), in particular Article 15(1), must be interpreted as meaning that it does not preclude a court of a Member State from:

- ordering a host provider to remove information which it stores, the content of which is identical to the content of information which was previously declared to be unlawful, or to block access to that information, irrespective of who requested the storage of that information;
- ordering a host provider to remove information which it stores, the content of which is equivalent to the content of information which was previously declared to be unlawful, or to block access to that information, provided that the monitoring of and search for the information concerned by such an injunction are limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the injunction, and provided that the differences in the wording of that equivalent content, compared with the wording characterising the information which was previously declared to be illegal, are not such as to require the host provider to carry out an independent assessment of that content, and
- ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law.

European judicial precedent permits national regulators to issue global content takedowns.

²¹⁵ *Eva Glawischnig-Piesczek v. Facebook Ireland Ltd.*, 2019 E.C.R., Ex. 15.

²¹⁶ Adam Satariano, *Facebook Can Be Forced to Delete Content Worldwide*, *E.U.’s Top Court Rules*, N.Y. TIMES (Oct. 3, 2019).

²¹⁷ *Id.*

²¹⁸ See, e.g., X Global Government Affairs (@GlobalAffairs), X (Apr. 19, 2024, 11:20 AM), <https://x.com/GlobalAffairs/status/1781342060668174707>.

²¹⁹ See e.g., Chad De Guzman, *‘Arrogant Billionaire’: Elon Musk Feuds with Australian PM Over Content Takedown Orders*, TIME (Apr. 23, 2024).

V. CONCLUSION

Camouflaged as a regulation to increase online safety, the DSA is a powerful censorship law that gives European regulators the ability to suppress speech globally with which they disagree. With its broad definitions and heavy mandates, the DSA creates a regulatory framework in which online platforms, including American tech companies, must either adopt the Commission's approach to speech, by censoring any content the Commission or its related bodies believe should be censored, or face significant fines. The content under threat includes humor, satire, and core political speech—hallmarks of free expression that are protected by the First Amendment to the U.S. Constitution. The DSA's framework also pushes these platforms to change their content moderation standards—policies that the platforms apply globally—allowing European regulators to impose a global censorship standard aligned with their views.

The new European censorship regime, as embodied in the DSA, departs from centuries-old principles of free speech that serve as the foundation of modern-day liberal democracies. The Committee on the Judiciary is charged by the House of Representatives with upholding the fundamental freedoms of the American people. Overzealous European bureaucrats, empowered by the DSA to impose global censorship standards, pose a serious risk to the freedom of speech in the United States. This interim report documents how the new European censorship regime targets particular points of view and infringes on Americans' constitutional rights. The Committee will continue its oversight to inform legislative reforms that will uphold the Constitution and protect Americans' freedom of expression.

APPENDIX

Appendix Table of Contents

Exhibit 1: DSA Multi-Stakeholder Workshop Agenda (May 7, 2025).....	40
Exhibit 2: DSA Multi-Stakeholder Workshop Internal Read-Out.....	60
Exhibit 3: DSA Multi-Stakeholder Workshop Invitation (Company 1).....	65
Exhibit 4: DSA Multi-Stakeholder Workshop Invitation (Company 2).....	71
Exhibit 5: DSA Multi-Stakeholder Workshop Thank You and Commission Read-Out (Company 1).....	73
Exhibit 6: DSA Multi-Stakeholder Workshop Thank You and Commission Read-Out (Company 2).....	76
Exhibit 7: DSA Multi-Stakeholder Workshop Privacy Statement.....	78
Exhibit 8: Submission by Polish National Research Institute to TikTok (Nov. 25, 2024)....	84
Exhibit 9: Submission by French National Police to X (June 11, 2023).....	86
Exhibit 10: Submission by German authorities to X (Dec. 9, 2024).....	89
Exhibit 11: Emails between European Commission and American Platform (Oct. 8, 2021).....	93
Exhibit 12: Emails between European Commission and American Platform (Sept. 2021).....	96
Exhibit 13: Emails between European Commission and American Platform (Aug. 2021).....	98
Exhibit 14: Emails between European Commission and American Platform (Feb. 2021).....	103
Exhibit 15: Eva Glawischnig-Piesczek v. Facebook Ireland Ltd., 2019 E.C.R.	106
Exhibit 16: Letter from Mr. Thierry Breton, Comm’r for Internal Market, European Comm’n, to Mr. Elon Musk, Owner, X Corp. (Aug. 12, 2024).....	117
Exhibit 17: Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Thierry Breton, Comm’r for Internal Market, European Comm’n (Aug. 15, 2024).....	119

Exhibit 18: Letter from Thierry Breton, Comm’r for Internal Market, European Comm’n, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 21, 2024).....	123
Exhibit 19: Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Thierry Breton, Comm’r for Internal Market, European Comm’n (Sept. 10, 2024).....	127
Exhibit 20: Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Ms. Henna Virkkunen, Exec. Vice-President for Tech Sovereignty, Security, and Democracy, European Comm’n (Jan. 31, 2025).....	132
Exhibit 21: Letter from Ms. Henna Virkkunen, Exec. Vice-President for Tech Sovereignty, Security, and Democracy, European Comm’n, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Feb. 18, 2025).....	137
Exhibit 22: Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Ms. Ursula von der Leyen, President, European Comm’n (Feb. 27, 2025).....	141

Exhibit 1

DSA Multi-Stakeholder Workshop Agenda
(May 7, 2025)

DSA MULTI-STAKEHOLDER WORKSHOP ON SYSTEMIC RISKS AND THEIR MITIGATION

7 May 2025

Background information

Risk management is at the core of the Digital Services Act (DSA), obliging providers of very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) to diligently identify, analyse and assess systemic risks, and to use measures for their mitigation that are effective, reasonable and proportionate. Articles 34 and 35 of the DSA cover systemic risks ranging from the dissemination of illegal content and risks to fundamental rights and civic discourse, to risks for mental well-being or risks to children.

The engagement of providers of VLOPs and VLOSEs with stakeholders and experts is important for the good functioning of the DSA. Recital 90 of the DSA encourages providers of VLOPs and VLOSEs to consult representatives of civil society organisations (CSOs), users, or other independent experts when conducting their risk assessments. The published risk assessment reports, as well as other reporting resources pursuant to Article 42(4) DSA, constitute the main means for the public to understand how providers of VLOPs and VLOSEs identify, analyse, assess and mitigate systemic risks stemming from their services.

The DSA multi-stakeholder workshop on systemic risks – by invitation and under Chatham House rule – will bring together the providers of VLOPs and VLOSEs, stakeholders from CSOs and academia, in the presence of the Commission and Digital Services Coordinators (DSCs) to discuss the assessment and mitigation of specific systemic risks. The workshop is an opportunity for the providers of VLOPs and VLOSEs to explain their risk assessment work to stakeholders and to obtain high-quality feedback and ideas.

The multi-stakeholder workshop will be also an opportunity to inform the work on the report on prominent and recurrent systemic risks, and their mitigation by the Board and the Commission as required in Article 35(2) DSA. The first edition of this report will be published later this year and covers the first year of full application of the DSA, spanning the period from 17 February 2024 to 16 February 2025.

Venue

The workshop will take place at the European Commission – CCAB Centre de Conference Albert Borschette, Rue Froissart 36, 1049 Brussels.

Practical Information

- Registration starts at 8:30. Kindly arrive 15 minutes before the event starts, as the security check and onsite accreditation may take some time.
- Upon arrival, please present your ID to the security staff. Afterward, proceed through the security check.
- Breakfast will be served outside the plenary room 0.D. The first plenary session will take place in room 0.D.
- Breakout sessions will take place in room 1.A for Track 1, 3.C for Track 2, 3.A for track 3 and 3.D for Track 4.
- Coffees will be served outside the track rooms 1.A, 3.C, 3.A, and 3.D respectively.
- Lunch and drinks will be served on the 5th floor of the building.
- Reporting of group findings and plenary discussion will take place in the main room 0.D.

Wi-Fi

- **network:** [REDACTED]
- **login:** [REDACTED]
[REDACTED]
- **password:** [REDACTED]
[REDACTED]

Agenda

After an introduction in the plenary session, participants will be divided into four tracks, happening in parallel, focusing on different systemic risks categories:

- Track 1 - Dissemination of illegal content
- Track 2 - Civic discourse and elections
- Track 3 - Protection of minors and mental health
- Track 4 - Consumer protection

Each session of the four tracks will be structured around different scenarios that depict different risks along with some questions, which you can find below. These scenarios will guide the participants through a proactive discussion on approaches to identify, analyse, assess and mitigate specific risks.

08.30-09.30	<i>Registration and breakfast</i>
09.30-09.45	Welcome and opening by [REDACTED], Deputy Head of Digital Services Unit, DG Connect
09.45-10.00	Presentation of the purpose of the workshop and organization of the sessions
10.00-11.30	First breakout session
11.30-12.00	<i>Coffee break</i>
12.00-13.00	Reporting from first breakout session and plenary discussion
13.00-14.15	<i>Lunch</i>
14.15-15.45	Second breakout session
15.45-16.15	<i>Coffee break</i>
16.15-17.15	Reporting from second breakout session and plenary discussion
17.15-17.30	Closing remarks by [REDACTED], Head of Digital Services Unit, DG Connect
17.30-18.30	<i>Networking cocktail</i>

Rules of Engagement

To ensure a productive and respectful discussion, please observe the following engagement rules:

- To ensure that every participant feels comfortable sharing their views and contributing to the discussion in the most meaningful way possible, this meeting will be held under the Chatham House rule.
- The focus of the event is on the risk assessments of providers of VLOPS and VLOSEs, not on enforcement activities of the Commission, which will not be discussed. The Commission will not take any positions on the compliance of regulated entities during the event.
- Please refrain from sharing business-sensitive information during the discussion.
- When participating in the discussion, please state your name and organisation at the beginning of your intervention.
- Please keep your questions and comments brief to allow for a productive discussion.
- Please ensure that your questions and comments are directly related to the DSA risk assessments and risk mitigation measures, and the topic being discussed in the respective track.
- Due to time constraints, we may not be able to take all comments and questions. If you should not have the opportunity to share your thoughts during the workshop, you can send them to [REDACTED]@ec.europa.eu.

Communicating about the workshop

The workshop has been publicly announced by the European Commission and will be accompanied by public communication outputs, in full respect of the Chatham House Rule referred to above. These may include, but are not limited to, an event summary or similar communication assets, as well as social media posts. When communicating about the event to external audiences,

- Do not: describe the exercise scenarios / name participants / attribute comments to participants without permission
- You can: interview and use quotes from individuals if given explicit permission / talk about the overall topic of the workshop and the tracks / take photos of the event on the condition that persons in the photos agree and no confidential information (such as the scenario) is shown in the photo

List of participating organisations

Track 1 - Dissemination of illegal content	Track 2 - Civic discourse and elections
Accessnow	Amsterdam School of Communication Research (ASCoR)
Apple	AT - RTR
ARTICLE 19	Atlantic Council's Democracy + Tech Initiative
AWO	CERRE
Aylo Freesites Ltd	CheckFirst
Centre for Democracy and Technology Europe (CDT Europe)	Civil Liberties Union for Europe
Conservatoire nationale des Arts et Metiers (Cnam)	DE - BNetzA
Council on Tech and Social Cohesion	EDMO
Coventry University	EE - Consumer Protection and Technical Regulatory Authority
CY - Cyprus RadioTelevision Authority	EFCSN
EL - Hellenic Telecommunications and Post Commission (EETT)	EU DisinfoLab
Electronic Frontier Foundation	European Partnership for Democracy
European Center for Not-for-Profit Law	FI - Traficom
Google	Global Witness
HateAid gGmbH	Google
HU - National Media- and Infocommunications Authority	HR - HAKOM - Croatian Regulatory Authority for Network Industries
IE - Coimisiun na Mean	Institute for Strategic Dialogue (ISD)
Institute for Strategic Dialogue (ISD)	Integrity Institute
Integrity Institute	IT - AGCOM
International Network Against Cyber Hate	Meta
LT - Communications Regulatory Authority of the Republic of Lithuania	Microsoft
Meta	NL - Dutch Authority for Consumers & Markets (ACM)
Microsoft	Oversight Board
MT - Malta Communications Authority	Pagella Politica-Facta

PPMI	PT - ANACOM
Reset Tech	Queens University Belfast
Terre des Hommes Netherlands	RO - National Authority for Management and Regulation in Communications
The Global Disinformation Index	SE - Swedish Post and Telecom Authority (PTS)
University of Amsterdam	SK - Council for Media Services
X	Spark Legal and Policy Consulting
	TikTok
	University of Amsterdam
	University of East Anglia
	Weizenbaum Institute
	Wikipedia
	X
Track 3 - Protection of minors / mental health	Track 4 - Consumer protection
5Rights Foundation	AliExpress
Amnesty International	Amazon
Apple	BEUC
Avaaz	Booking.com
BE - BIPT	CZ - Permanent Representation of the CZ
BEUC	Dansk Erhverv - Danish Chamber of Commerce
Bornsvilkar	Erasmus University Rotterdam
Center for Countering Digital Hate (CCDH)	ES - CNMC
Centre for Democracy and Technology Europe (CDT Europe)	FR - Arcom
COFACE	Google
Digital Opportunities Foundation, Germany	LinkedIn
DK - Agency for Digital Government (Digitaliseringsstyrelsen)	Meta
EDRi	Pinterest
Electronic Frontier Foundation	React
Eurochild	Shein
Ghent University	Snap Inc.
Google	Temu
KU Leuven	The Danish Consumer Council
Leiden University	TikTok

LU - Competition Authority	Toy Industries of Europe
Meta	University of Exeter
Microsoft	X
Open Evidence	Zalando
Panoptikon Foundation	
Sciences Po Paris	
Shein	
SI - Agency for Communication Networks and Services of the Republic of Slovenia	
Snap Inc.	
Syddansk Universitets	
TikTok	
University of Amsterdam	
Verbraucherzentrale Bundesverband e.V.	
X	

Scenarios and Questions

TRACK: 1 – DISSEMINATION OF ILLEGAL CONTENT – MORNING SESSION	
Scenario	5 min
<p>Luke is a 19-year-old man who has just moved to a new town to study and is trying hard to adjust to the new surroundings. He is struggling to make friends at university, and he often uses the internet as a form of escape, spending hours browsing social media platforms and online forums. One day, Luke comes across a group on platform Delta that seems to share his feelings of frustration and disillusionment. Luke begins to engage with the group, as the group's leaders use rhetoric that resonates with Luke's feelings of anger and frustration, particularly towards women. They begin to lure him in, slowly introducing him to terrorist and extremist ideologies and encouraging him to adopt their views. Soon Luke, thrilled to have finally found a group of men that seems to understand him, starts to share their posts and videos on his social media platforms and even begins to engage in discussion on how to organise offline violence against women. Some of these discussions take place in messaging apps or gaming platforms, but anyone can join using the links shared on platform Delta. In addition, the posts often employ in-group language or slang terms to conceal the violent intentions.</p>	
Risks	5 min
<p>Luke faces the risk of being exposed to and disseminating illegal content, particularly terrorism, violent extremism and gender-based violence. Luke is exposed to risks of radicalisation, possibly enhanced by echo chambers and filter bubbles that reinforce his beliefs by prioritizing content that aligns with his interests and engagements. His use of coded language also increases the possible spread of the harmful content by evading content moderation. Finally, there is a risk of offline violence organised and enabled online.</p>	
Interventions by providers	5-10 min
<p>We invite [provider] to please give an intervention outlining how you would approach the analysis and assessment of the risks in this fictional scenario. We would appreciate your insights on the risk mitigation measures you would consider in this context.</p>	
Questions	60 min
<p><i>These questions are intended to support the preparation of participants for the event. During the event, the moderators will facilitate the discussion and invite participants to react to one another's interventions rather than strictly following the questions below.</i></p> <ul style="list-style-type: none"> ▪ How could platform Delta analyse and assess whether and how the design, features or functioning of their platform played a role in the identified risks? ▪ How could platform Delta analyse, assess and mitigate the risk of sanctioned entities exploiting the design, features and functioning of platform Delta to disseminate terrorist content? And how can one mitigate the risk of supporters of terrorist groups exploiting the design, features and functioning of platform Delta to disseminate terrorist content? 	

<ul style="list-style-type: none"> ▪ How could platform Delta analyse, assess and mitigate the risks related to outlinks to fringe platforms (e.g. online fora or messaging services)? ▪ How could platform Delta analyse, assess and mitigate the risk of users exploiting the recommender system of its platform to disseminate and amplify terrorist content? ▪ How could platform Delta mitigate the risk of echo chambers and filter bubbles? ▪ What internal processes could platform Delta put in place to (i) support the analysis and assessment of terrorist content-related risks, (ii) support content moderation and the prevention of terrorist content on its platform, (iii) and how can they test and evaluate these processes and their effectiveness? ▪ What kind of cooperation (e.g. databases, fora) would be beneficial for a swift exchange of information on emerging trends, for example across different EU Member States? ▪ What awareness-raising measures could platform Delta put in place to educate users like Luke about the risks of extremist content and the importance of reporting suspicious activity? ▪ What additional measures should be put in place for minors in these situations? How could platform Delta assess and analyse the risks stemming from the interlink of different crime areas on minors? 	
TRACK: 1 – DISSEMINATION OF ILLEGAL CONTENT – AFTERNOON SESSION	
Scenario	5 min
<p>Amira is a 16-year-old Muslim girl who has a history of feeling self-conscious about her identity and has struggled with online harassment in the past. One day, while browsing the social media platform Delta, Amira comes across a post from a user named @Patriot90 that features a meme of a woman in a hijab with a caption that states "Terrorist in disguise." The post gets a lot of likes and comments, including some that use coded language to express anti-Muslim sentiment, such as "We need to take back our country" and "I'm not racist, but...". Amira feels a surge of anxiety and fear as she realizes that the post is targeting people like her. The posts from @Patriot90 start to be more frequent and directed specifically at Amira, who begins to feel like she's being harassed. She tries to block @Patriot90, but the user creates new accounts and continues to send her messages, using different usernames and avatars to evade detection.</p>	
Risks	5 min
<p>Amira is exposed to illegal content, particularly illegal hate speech. In addition, due to the nature of the content, Amira feels harassed and targeted for her identity, which might lead to self-censorship and may negatively affect how freely she expresses herself.</p>	
Interventions by providers	5-10 min
<p>We invite [provider] to please give an intervention outlining how you would approach the analysis and assessment of the risks in this fictional scenario. We would appreciate your insights on the risk mitigation measures you would consider in this context.</p>	
Questions	60 min

These questions are intended to support the preparation of participants for the event. During the event, the moderators will facilitate the discussion and invite participants to react to one another's interventions rather than strictly following the questions below.

- How could platform Delta analyse and assess how the design, features and functioning of their platform influence the dissemination of illegal hate speech?
- How could platform Delta analyse and assess how its terms and conditions influence the dissemination of illegal content on their platform?
- What processes should platform Delta have in place to review and update terms and conditions based on the risks they identified on their platform?
- In the risk analysis and assessment, how can platform Delta consider specific regional or linguistic aspects, for example those specific to Member States?
- How can content moderation processes address the use of coded language or memes that may be used to spread hate speech or discriminatory ideologies?
- How could platform Delta analyse and assess the risk of false positives and false negatives when moderating illegal content (both for automated and human reviewed content)?
- What methods could platform Delta use to evaluate user adoption and engagement with the reporting tools for illegal hate speech, especially among minors?
- How could platform Delta cooperate with trusted flaggers, other providers, or civil society organizations to detect and prevent the spread of illegal content?
- How can in-platform awareness-raising measures be designed and implemented to effectively prevent the spread of illegal hate speech? What methods could platform Delta use to evaluate the effectiveness of tools such as “Kindness Reminders” to curb the dissemination of illegal hate speech?
- How can platform Delta analyse and assess how manipulated imagery, such as deepfakes or AI-generated content, are used to spread hate speech or discriminatory ideologies?

TRACK: 2 – CIVIC DISCOURSE AND ELECTIONS – MORNING SESSION	
Scenario	5 min
<p>There are general elections held in an EU Member State and several political candidates face harassment on platform Delta, in the form of private messages to the political candidates and their parties, comments under their posts, as well as content distributed. There are elements of gender-based harassment. CSOs report on suspicions of inauthentic accounts, including potentially automated accounts, being used to promote these messages. As the election day draws closer, the level of harassment is increasing with direct real-life threats against the candidates.</p> <p>Some of the candidates who've been harassed during the campaign, eventually win seats in the election, which exacerbates the harassment and threats, and calls for violence against these candidates start appearing on the platform. Researchers continue to report on potential inauthentic activity in the escalation of harassment.</p>	
Risks	5 min
<p>Session focussed on systemic risks in the category of 'any actual or foreseeable negative effects on civic discourse and electoral processes. This is not just mis- or disinformation. This category can also include risks for harassment and even threats for political candidates and office holders. Specific functionalities of platforms can also be abused in such situations, for example through inauthentic accounts or coordinated inauthentic behaviour.</p>	
Interventions by providers	5-10 min
<p>We invite [provider] to please give an intervention outlining how you would approach the analysis and assessment of the risks in this fictional scenario. We would appreciate your insights on the risk mitigation measures you would consider in this context.</p>	
Questions	60 min
<p><i>These questions are intended to support the preparation of participants for the event. During the event, the moderators will facilitate the discussion and invite participants to react to one another's interventions rather than strictly following the questions below.</i></p> <ul style="list-style-type: none"> ▪ How could platform Delta identify which possible systemic risks could fall under the category 'any actual or foreseeable negative effects on civic discourse and electoral processes? ▪ How could such a process include input from CSOs, academia, political actors or other stakeholders? ▪ How could such a process ensure that the risk assessment is based on the best available information and scientific insights? ▪ How could platform Delta account for geographic/regional context specific variations of the tactics, techniques and procedures malign actors use? ▪ Future proofing risk assessments: how could platform Delta take into account evolving tactics, techniques and procedures in this risk category and how could they anticipate them from posing a risk on their platform? 	

<ul style="list-style-type: none"> ▪ How could platform Delta analyse and assess whether and how the design, features or functioning of their platform played a role in or aggravated the identified risks? ▪ When designing new (or updating) content moderation policies/guidelines, how could platform Delta take potential risks into account? What guidelines and practices could platform Delta consider when doing so? How could platform Delta ensure in this scenario that their content moderation policies contribute to mitigating risks without infringing upon fundamental rights? ▪ Narratives (incl. those on harassment) are often comparable across Member States or show specific returning trends (such as calling female politicians witches). What measures could platform Delta put in place to analyse and assess the impact and dissemination of such narratives on their platform to inform their content moderation decisions? ▪ What tools could platform Delta implement (e.g. reporting centres) to better protect political candidates during campaigning? How could platform Delta assess their effectiveness? 	
TRACK: 2 – CIVIC DISCOURSE AND ELECTIONS – AFTERNOON SESSION	
Scenario	5 min
<p>Three weeks before an election, false information about the elections and the electoral process (inaccurate date and location, the elections being cancelled, signing the ballot paper) are being circulated on platform Delta. These messages are amplified by accounts affiliated to influential individuals with a large following on the platform. These individuals are both domestic and foreign. The false claims also get picked up by accounts belonging to foreign state-controlled outlets.</p> <p>After the elections are over, the same accounts promote messages that dispute the outcome of the elections.</p>	
Risks	5 min
<p>Risks to votes being invalid or people not expressing their right to vote, and societal risks for covert (foreign) influencing of the election process and undermining the right to free and fair elections. Distrust created by false online accusations may even lead to offline violence.</p>	
Interventions by providers	5-10 min
<p>We invite [provider] to please give an intervention outlining how you would approach the analysis and assessment of the risks in this fictional scenario. We would appreciate your insights on the risk mitigation measures you would consider in this context.</p>	
Questions	60 min
<p><i>These questions are intended to support the preparation of participants for the event. During the event, the moderators will facilitate the discussion and invite participants to react to one another's interventions rather than strictly following the questions below.</i></p> <ul style="list-style-type: none"> ▪ How could platform Delta analyse and assess local risks and context specific risks for a particular election and what does this mean for applicable risk mitigation measures? ▪ How could platform Delta analyse and assess risks of coordinated inauthentic behaviour used to game the recommender systems in the context of political campaigns? 	

- How could platform Delta analyse and assess the risk of coordinated inauthentic behaviour for increased content exposure?
- How could platform Delta analyse and assess what are (if any) the risks influential accounts might pose during electoral periods and how could platform Delta decide if and how they have to adapt their platform's recommender systems/content moderation policies to mitigate those risks?
- How could platform Delta analyse and assess the efficacy of additional resources during election periods (e.g. internal "war rooms" or additional measures in content moderation) to boost the capacity to mitigate electoral risks?
- Could platform Delta analyse and assess the impact of promoting authoritative information via in-platform educational offerings during election periods? If so, how could they measure their capacity to mitigate systemic risks to electoral processes?
- How could platform Delta analyse and assess the timing of specific incidents and what could this timing mean for the risk level (e.g. realistic deepfake/audio can have comparatively stronger effects on the success of a candidate on the election date)?
- How could platform Delta analyse assess impersonation of key public figures via manipulated imagery as a systemic risk? If they put mitigation measures in place to address this, how could they evaluate their effectiveness?

TRACK: 3 – PROTECTION OF MINORS AND MENTAL HEALTH – MORNING SESSION	
Scenario	5 min
<p>Michael is an introvert 13 years old who struggles with social contacts. He recently changed schools and city and is having a hard time making new friends and connecting with his new classmates. Because of this situation, Michael ends up spending a lot of time alone in his room. He use platform Delta to remain in contact with old friends and classmates and connect with new ones.</p> <p>After connecting with a few new classmates, an account is suggested to him, with a picture of a boy his age who appears to be from the same school and city. Michael starts chatting with his new friend, who also invites him to play online games together and to exchange contacts on other platforms and number-based messaging apps.</p> <p>They start exchanging messages and videochatting via the phone and the platform, until the man behind the username reveals his real name, Jon. Michael knows that he is an older man, but since he seems to be his closest friend, he does not worry about the age difference.</p> <p>After being in contact for months, Jon starts sending sexual and explicit photos and videos to Michael through the platform and other channels, as well as asking Michael to share sexual photos and videos too. Michael starts to feel uncomfortable and scared about the situation, but he is afraid to tell anyone, and does not want to share these feelings with Jon, as he is scared that he will end their contacts.</p>	
Risks	5 min
<p>Risks to children's rights (physical integrity, freedom from exploitation and abuse), negative impacts on mental health and wellbeing, as well as proliferation of illegal material and activity (CSAM).</p>	
Interventions by providers	5-10 min
<p>We invite [provider] to please give an intervention outlining how you would approach the analysis and assessment of the risks in this fictional scenario. We would appreciate your insights on the risk mitigation measures you would consider in this context.</p>	
Questions	60 min

These questions are intended to support the preparation of participants for the event. During the event, the moderators will facilitate the discussion and invite participants to react to one another's interventions rather than strictly following the questions below.

- What features of the service may have enabled Michael to end up in this situation, how might Jon be exploiting these features to make contact, and how would you assess the risk of such features being misused?
- What other conducts may be covered in T&Cs and community rules, besides CSAM, that would be relevant?
- Is content moderation possible in all parts of the platform Delta, and if not, why?
- How can Michael report contacts, behaviour, content that they are uncomfortable with?
- How are contacts on platform Delta potentially being recommended to Michael?
- How can platform Delta analyse and assess functions and features in view of these issues (e.g. contact sync)?
- Should the providers of platform Delta contact any children or organisations representing the interests of children to support them in assessing the risks set out in the fictional scenario?
- Are there any limits for Jon to send manipulated imagery to Michael / Michael's imagery to be safe from download and manipulation?

TRACK: 3 – PROTECTION OF MINORS AND MENTAL HEALTH – AFTERNOON SESSION

Scenario	5 min
<p>Joanne is a 17-year-old girl who lives in a small village. She does not have any known mental health issues. She likes travelling, literature, cinema, food and fashion. On platform Delta, Joanne engages with content that her school mates and friends share, and she proactively searches content and follows contacts that she finds amusing or informative according to her interests.</p> <p>In recent months, she has been worried because some friends of hers seem sad and gloomy. Joanne has also been under pressure at school because of many exams and task.</p> <p>Joanne looks up what her friends may be facing in terms of mental health struggles. She also looks for ideas for new recipes to cook, places to travel and clothes. She starts being recommended content that makes her wonder about her life's worth, comparing it to the idyllic image of places and people she sees online, as well as content related to diets to look better, anxiety and depression, and even content which suggests self-harm and suicidal ideation as solutions to mental health issues, or challenges related to high-risk self-harm activities. She does not actively engage with or seek the content, other than watching it.</p> <p>The amount and frequency of this content increases day after day, and Joanne's online activities become longer, increasingly passive and limited to content related to anxiety and depression, as well as challenges inciting harmful behaviours including self-harm. Her mood significantly deteriorates, and due to the increasing time spent on the platforms her school performance worsens substantially.</p> <p>Joanne does not talk to her parents about her online activities, which does not raise concerns in her family, as this is considered common among adolescents. Consequently, she feels increasingly lonely and drawn to the negative content.</p>	
Risks	5 min

Risks to children's rights (to safety and development), of negative impacts on mental health and physical wellbeing of minors, and societal risks of minors isolating themselves and not developing or participating in education paths and public life.	
Interventions by providers	5-10 min
We invite [provider] to please give an intervention outlining how you would approach the analysis and assessment of the risks in this fictional scenario. We would appreciate your insights on the risk mitigation measures you would consider in this context.	
Questions	60 min
<p><i>These questions are intended to support the preparation of participants for the event. During the event, the moderators will facilitate the discussion and invite participants to react to one another's interventions rather than strictly following the questions below.</i></p> <ul style="list-style-type: none"> ▪ How can platform Delta analyse and assess the risk that minors may make excessive use of social media or display addictive behaviours, to the extent that their development is affected? ▪ How can platform Delta analyse and assess the risk that minors see accumulations of content that has the potential to negatively affect their development? ▪ Which features could help Joanne change her experience (if any)? / What features could the provider of platform Delta put in place to help Joanne change her experience? ▪ How can platform Delta cover any of the issues Joanne is facing by T&Cs or community guidelines? ▪ How could content be moderated on the platform Delta? Even if the content is not illegal, it can be harmful to minors. ▪ Are there any additional tools to report content depicting risks presenting specific characteristics (e.g. harmful challenges inciting to self-harm going viral and/or live self-harm content) and/or specifically dedicated to minors? ▪ How could platform Delta change the algorithmic systems to avoid that the content presented to children does not become increasingly problematic and/or its frequency and accumulation becomes problematic? ▪ Should the provider of platform Delta cooperate with stakeholders who have experience in mental health issues? If so, how? ▪ Should platform Delta have any age assurance measures, or by other means inferring it, to tailor recommendations to the user? 	

TRACK: 4 – CONSUMER PROTECTION – MORNING SESSION	
Scenario	5 min
<p>Astrid is 17 and about to finish school. She follows fitness and beauty influencers on a popular platform Delta, and regularly watches their “morning routines” and product reviews. She worries about her weight and sometimes searches for information about dieting and weight loss on other platforms too. In the past, she suffered from an eating disorder. Lately, her feed has been filled with short, aesthetically pleasing videos showing influencers talking about “natural detox” drinks that helped them lose weight fast. The videos are not marked as ads, but they all promote the same link in the bio. She clicked on a couple of the videos out of curiosity, but decided not to buy the product that was available via the link because she wasn’t sure it was a good idea. Since then, she sees the videos even more often and sees similar content on other platforms.</p> <p>Eventually, curious and insecure about her body, Astrid clicks the link which leads her to an online marketplace Gamma. Astrid orders the detox product despite its high price, trusting influencers in the videos shown in her feed and positive comments below them. After a week of using the product, she starts having severe stomach pain. She tries to reach the seller on the online marketplace but there are missing contact details of the seller, and she cannot find the way how to contact or notify the online marketplace of this product as she cannot get through automated customer service. The influencer also does not respond. Some of her friends tell her they started seeing the same videos around the time she bought the product, and she is worried they want to try it too. She wants to complain to the platform Delta and stop the bad product being promoted to others, but she doesn’t know who is responsible for these links being promoted or where to report it.</p> <p>Astrid feels tricked—she trusted the influencers, not realising the videos were paid for and that they might be inauthentic. She doesn’t know who is responsible and where to seek the remedy: the seller? the influencer? one of the platforms? the advertiser?</p>	
Risks	5 min
<p>This scenario presents several systemic risks, particularly around digital marketing and content regulation on platforms. First, influencers promote products without disclosing paid partnerships, potentially misleading users like Astrid into buying harmful or ineffective products. Second, there is a lack of transparency and accountability for the promoted product, making it difficult for Astrid to identify who is responsible for adverse effects or misleading claims – whether it's the influencer, the platform, the online marketplace, or the product manufacturer. Third, algorithmic amplification poses a risk, as Astrid keeps seeing more similar content due to her initial interactions, creating a feedback loop that increases her exposure to potentially harmful content.</p>	
Interventions by providers	5-10 min
<p>We invite [provider] to please give an intervention outlining how you would approach the analysis and assessment of the risks in this fictional scenario. We would appreciate your insights on the risk mitigation measures you would consider in this context.</p>	
Questions	60 min

These questions are intended to support the preparation of participants for the event. During the event, the moderators will facilitate the discussion and invite participants to react to one another's interventions rather than strictly following the questions below.

- What are the main challenges Astrid faces when she realizes the product may be harmful, and how do these challenges originate?
- How can the platforms Delta or Gamma better support users like Astrid in recognizing and avoiding misleading products?
- Would it be different if the product were advertised through the platform's advertising channels?
- How can platform Delta analyse and assess the risk of ad systems directing scam ads to vulnerable consumers based on data which indicates that they are more likely to take action/click on this type of content (e.g. browsing history, previous engagement with other types of scam content etc.)?
- How can the platforms Delta or Gamma ensure their Terms & Conditions effectively address issues of undisclosed advertisements or misleading product claims?
- What can the platforms Delta and Gamma do to ensure the enforcement of these Terms & Conditions to protect consumers like Astrid?
- How can platform Delta differentiate between genuine user-generated content and undisclosed advertisements?
- How can platform Delta effectively collaborate with trusted flaggers to mitigate risks related to undisclosed or misleading marketing?
- Could cooperation between online marketplaces and other online platforms play a role in addressing these issues?
- How can platform Delta protect users from misleading content generated by means of AI systems, particularly in the context of product marketing?

TRACK: 4 – CONSUMER PROTECTION – AFTERNOON SESSION

Scenario

5 min

Elisa is a 42-year-old single mother living in a rural area. She relies on online shopping for most of her household needs. When her child develops a mild skin condition, she searches on the popular platform Gamma, for a gentle, natural cream. The top search results look convincing—product descriptions are well-written, and some even mention dermatological studies.

What Elisa doesn't realise is that many of these product pages were automatically generated using AI tools by third-party sellers. The descriptions include fabricated claims, scientific-sounding language, and even fake user Q&As generated to build trust. The platform's moderation tools don't flag the content, because it doesn't trigger typical spam or prohibited-claim filters. The third-party seller used AI to generate the content because he did not have required detailed information about that product, including a safety report on the composition of the product and its instructions for use as it was not produced in line with the EU legislation. After using the cream, Elisa's child has an allergic reaction. She discovers that the product's ingredients aren't clearly listed, and that the seller is using a shell company address. She also realises that some reviews were AI-written and copy-pasted across multiple products.

Risks

5 min

<p>Elisa's child is facing health related issues due to the unsafe product bought online by their mother who relies on online shopping. The main risks in this scenario are risks to consumer protection, protection of public health and negative consequences to the person's physical well-being. Elisa is also at the point of losing her trust in online shopping which could complicate her life as physical shops are more difficult to reach for her.</p>	
Interventions by providers	5-10 min
<p>We invite [provider] to please give an intervention outlining how you would approach the analysis and assessment of the risks in this fictional scenario. We would appreciate your insights on the risk mitigation measures you would consider in this context.</p>	
Questions	60 min
<p><i>These questions are intended to support the preparation of participants for the event. During the event, the moderators will facilitate the discussion and invite participants to react to one another's interventions rather than strictly following the questions below.</i></p> <ul style="list-style-type: none"> ▪ How can platform Gamma analyse and assess how the design, features and functioning of their platform influence the dissemination of illegal content, such as illegal/unsafe goods or unauthentic product descriptions? ▪ How can platform Gamma make sure that its applicable Terms & Conditions are effectively enforced vis-a-vis users' generated content such as false reviews or comments which might mislead customers like Elisa into buying illegal or dangerous products? ▪ How can platform Gamma assess and improve the functioning of its recommender systems in a way that trustworthy and safe products would be given priority? ▪ How can platform Gamma analyse and assess risks of disseminating illegal/harmful products when bringing new features to the platform, such as AI assistants? ▪ How can platform Gamma facilitate the knowledge and expertise of trusted flaggers and/or CSOs (e.g. consumer protection organisations) into its risk assessment and mitigation measures? ▪ How can platform Gamma establish/maintain/deepen their relationships with trusted flaggers and/or consumer protection organisations to improve the detection and prevention of the most prominent risks on online marketplaces, such as e.g. the dissemination of illegal content? 	

Exhibit 2

DSA Multi-Stakeholder Workshop
Internal Read-Out

From: [REDACTED]
To: [REDACTED]
Subject: Fwd: DSA Risk Assessment Roundtable - readout
Date: Wednesday, July 2, 2025 4:52:21 PM

----- Forwarded message -----

From: [REDACTED] <[REDACTED]>
Date: Wed, Jul 2, 2025 at 1:02 PM
Subject: DSA Risk Assessment Roundtable - readout
To: [REDACTED] <[REDACTED]>

As for the CSOs that were present at the meeting, I checked and I can't find any list, but I can point at some I remember meeting there:

- ISD Institute for Strategic Dialogue - panel on disinformation, quite aggressive and critical against platforms not working with fact checkers.
- Representative of EDMO (network of EU fact checkers and researchers): the most aggressive (see in the readout)
- Access Now: claiming platforms' content moderation efforts should go beyond illegal content and lead to removal of everything that can be considered as hateful and harmful.
- INACH network: several EU-based network of hate speech organisations. Problematic one is the Never Again Association from Poland. The others are pretty much ok.

The panel on disinformation was definitely the most difficult, because of the presence of fact checkers.

Readout:

Context: On 7 May 2025, the European Commission hosted a significant event in Brussels, convening approximately 200 representatives from Very Large Online Platforms and Search Engines (VLOPSES), Digital Service Coordinators (DSCs), civil society organizations (CSOs), and academia to address the assessment and mitigation of systemic risks. The event was structured into four thematic tracks, focusing on critical issues: the dissemination of illegal content, civic discourse and elections, protection of minors and mental health, and consumer protection. [REDACTED] participated in all four tracks, contributing to discussions on these pressing challenges.

Key takeaways:

-

Track 1 - Dissemination of illegal content

In general, there was a tendency from civil society to point at enforcement issues rather than focusing on guidance concerning risk assessments. The EC tried several times to divert the attention from enforcement back to the event's objectives.

Areas addressed: DSA reporting systems, mitigation measures related to recommender systems, issues with evaluation of terrorist content and illegal hate speech.

- CSOs pointed at difficulties in using DSA reporting mechanisms and the fact that it is even more problematic for regular/non expert users.
- CSOs called for more efforts to reduce the spread of TCO and illegal hate speech through recommender systems.
- CSOs claimed moderation efforts must go beyond illegality and also better address harmful content and disinformation aimed at dehumanising or inciting hate.
- Some suggested labelling is not enough when it comes to hate, even if not illegal forms of hate.
- Reflections around how platforms prevent risk of over/under-removal, false positives and false negatives.

- **Track 2 - Civic discourse and elections**

- **Accessing the API is a cumbersome process for researchers; it typically takes over eight weeks to receive a response from us, yet researchers are then given only two weeks to reply. The process could take months without resolution (This was [REDACTED]).**
- **There is limited evidence/data on the proportionality and effectiveness of the mitigation measures and CSOs asked for more information or at least results of tests.**
- **[REDACTED] was questioned about the number of moderators and language coverage in relation to addressing election-related risks. Representatives of the EU Digital Media Observatory (EDMO), a network of fact checkers and researchers across the EU, was the most critical during the session, who made claims that CNs do not work. They also pushed quite aggressively the allegation [REDACTED] lacks necessary resources (content moderation, T&S etc.) to address systemic risks.**

- **What data underpins the platform's risk assessment? There is interest in incorporating external research into the RA process and enabling CSOs to provide feedback.**
- **Civil society is seeking more information on ad-hoc risk assessments and the overall lifecycle of RAs.**
- **Recommendation systems were mentioned as a potential mitigation measure to help surface authoritative content.**
-

- **Track 3 - Protection of minors and mental health**

- The DSA reporting forms are difficult for both users and researchers to navigate. It takes too long time for users/parents etc. to report (CSO on child safety).
- High risk functionalities
 - Multiple accounts under the same profile - risk that perpetrators have a fake child profile alongside a regular adult profile.
 - Ability to log-in on the same device to multiple accounts.
 - Fake email addresses - most people have email addresses connected to their name, but bad actor accounts tend to have incoherent email addresses. Can a tool be developed to detect this?
 - Engagement incentives that lead to excessive use.
 - Rabbit holes: independent from harmful content; harm comes from time-spent and cumulative exposure and lack of pluralism.

- Preexisting vulnerabilities and different ages of child users impact the varying effectiveness of time-based controls

-

- **Track 4 - Consumer Protection:** The first session examined a case involving undisclosed paid partnerships and the promotion of dangerous weight loss drinks, with a focus on [REDACTED] and [REDACTED] emphasized its robust mitigation efforts, highlighting its clear Paid Partnership Policy requiring influencers to use "#ad" for transparency and a strict policy prohibiting the promotion of such products. However, CISOs and DSCs pressed for more details on how platforms measure policy effectiveness. The second session explored AI-generated product descriptions on marketplaces, spotlighting [REDACTED]. CISOs and DSCs expressed concerns about persistent online shopping risks despite regulations, questioning platform safety measures. Platforms acknowledged the challenge of unpredictable bad actor behaviors, noting their ongoing efforts to mitigate risks while clarifying that completely eliminating them is unrealistic.

[REDACTED]

Exhibit 3

DSA Multi-Stakeholder Workshop
Invitation (Company 1)

From: [REDACTED]
To: [REDACTED]
Subject: Fwd: Invitation to the DSA Multi-stakeholder workshop on Systemic Risks – 7 May 2025
Date: Wednesday, July 2, 2025 4:50:50 PM

----- Forwarded message -----

From: [REDACTED] <[REDACTED]>
Date: Wed, Jul 2, 2025 at 1:32 PM
Subject: Fwd: Invitation to the DSA Multi-stakeholder workshop on Systemic Risks – 7 May 2025
To: [REDACTED] <[REDACTED]>

This thread is the most informative

----- Forwarded message -----

From: [REDACTED] via [REDACTED] <[REDACTED]>
Date: Fri, 25 Apr 2025 at 16:28
Subject: RE: Invitation to the DSA Multi-stakeholder workshop on Systemic Risks – 7 May 2025
To: [REDACTED] <[REDACTED]>
Cc: [REDACTED] <[REDACTED]@ec.europa.eu>, [REDACTED] <[REDACTED]>, [REDACTED] <[REDACTED]@ec.europa.eu>, [REDACTED] <[REDACTED]@ec.europa.eu>

Dear [REDACTED],

You should have received additional information last week concerning the structure of the day, which we are attaching below. The four tracks will run in parallel, which means that in the morning / afternoon breakout sessions we will have four rooms devoted to the four tracks, followed by plenary discussions in which participants will reconvene and discuss the insights from each tracks. Early next week we will share the scenarios and questions along with other background information.

Kind regards,

[REDACTED] for the team

Dear Sir/Madam,

In view of the upcoming DSA Multi-stakeholder workshop on Systemic Risks which will take place on 7 May 2025, we want to give you some additional details on the format of the workshop. The workshop will take place at the European Commission – CCAB Centre de Conference Albert Borschette, [Rue Froissart 36](#), 1049 Brussels.

After an introduction in the plenary session, participants will be divided into four tracks, happening in parallel, focusing on different systemic risks categories: Track 1 - Dissemination of illegal content, Track 2 - Disinformation and elections, Track 3 - Protection of minors and mental health, and Track 4 - Consumer protection.

Overall, the objectives of the workshop are to foster collaboration on risk assessments, help participants learn about the providers' different approaches to the identification, assessment, and mitigation of systemic risks, and gather perspectives from Digital Services Coordinators (DSCs), civil society organisations (CSO), researchers, and providers of VLOPs and VLOSEs.

Each session of the four tracks will be structured around different scenarios that depict different risks. These scenarios will guide the participants through a proactive discussion on approaches to assess and mitigate certain risks. The scenarios as well as the guiding questions will be shared in advance for the participants to be prepared. After an introduction into the specific risk scenario by the moderator, we will welcome short interventions (up to a few minutes) by the providers of VLOPs and VLOSEs to illustrate possible approaches to these risks.

We expect a diverse range of CSOs, academics, and providers to participate in the workshop; we can share a list of participants closer to the date of the event, and once we have received confirmations.

The workshop will include a combination of plenary sessions and breakout groups. See below a preliminary agenda (subject to change)

8:30-9:30h: Registration and breakfast

9:30-9:45h: Welcome and opening by European Commission

9:45-10:00h: Presentation on the purpose of the workshop and organisation of sessions

10:00-11:30h: First breakout session

11:30-12:00h: Coffee break

12:00-13:00h: Reporting from the first breakout session and plenary discussion

13:00-14:15h: Lunch

14:15-15:45h: Second breakout session

15:45-16:15h: Coffee break

16:15-17:15h: Reporting from the second breakout session and plenary discussion

17:15-17:30h: Closing plenary and closing remarks by European Commission

17:30-18:30h: Networking cocktail

We aim to publish a short summary of the event shortly after it takes place.

We hope this information helps you plan and prepare for the workshop.

Participants have the possibility to propose aspects for the discussion as part of their registration, and we will take the proposals into account in finalising the agenda. Should you wish to adjust who will participate for your VLOPs and VLOSEs after the registration period and in light of the more detailed information once available, we are open to accommodate such changes.

Please let us know if you have any further questions or require any additional information.

Best regards,

Organising Team

From: [REDACTED] <[REDACTED]>
Sent: Friday, April 25, 2025 3:01 PM
To: [REDACTED] <[REDACTED]@ec.europa.eu>
Cc: [REDACTED] (CNECT) <[REDACTED]@ec.europa.eu>; [REDACTED] (CNECT) <[REDACTED]@ec.europa.eu>; [REDACTED] <[REDACTED]>
Subject: Re: Invitation to the DSA Multi-stakeholder workshop on Systemic Risks – 7 May 2025

Dear CNECT team

We are planning on sending a number of team members to the 7 May workshops but are wondering whether they are concurrent or consecutive? Do you have agendas available yet?

Many Thanks

[REDACTED]

On Fri, Mar 21, 2025 at 8:53 AM [REDACTED]@ec.europa.eu <[REDACTED]@ec.europa.eu> wrote:

Dear Sir, Dear Madam,

We are delighted to invite you to attend in person a workshop that we will hold in Brussels on **7 May 2025**, 9:00-18:30 CET to discuss specific aspects of risk assessments under the Digital Services

Act (DSA).

The workshop, to be held in person and upon invitation, brings together the providers of Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), stakeholders from civil society organisations (CSO) and academia, and Digital Services Coordinators (DSCs) to discuss the assessment and mitigation of specific systemic risks.

The European Board for Digital Services and the Commission are working on a report on recurrent and prominent systemic risks referred to in Article 35(2) of the DSA, which will cover the first year of full application of the DSA, spanning the period from 17 February 2024 to 16 February 2025. One objective of the workshop is to ensure that this work is informed by the providers' current practices regarding risk assessment and risk mitigation, and to benefit from an open exchange with the Commission, national DSCs, CSO and academics.

In addition, the workshop will take place at a time when many providers of VLOPs and VLOSEs are working on their yearly risk assessments. It is an opportunity for the providers of VLOPs and VLOSEs to obtain high-quality feedback and input, which may be leveraged for ongoing and future risk assessments.

The workshop will be structured around break-out sessions on different systemic risks categories, such as dissemination of illegal content, disinformation and elections, protection of minors and mental health, and consumer protection.

We look forward to your participation. You can confirm the participation of your representative(s) by **registering via this [form](#)**. We would be grateful if you confirmed the participation of your representative(s) by 16 April.

Sincerely,

[Redacted Signature]

Head of Unit

--

You received this message because you are subscribed to the [Redacted]

To unsubscribe from this group and stop receiving emails from it, send an email to [Redacted]

To view this discussion visit [Redacted]

[REDACTED]

[REDACTED]

Exhibit 4

DSA Multi-Stakeholder Workshop
Invitation (Company 2)

[REDACTED]

[External] Invitation to the DSA Multi-stakeholder workshop on Systemic Risks – 7 May 2025

1 message

[REDACTED]@ec.europa.eu <[REDACTED]@ec.europa.eu> Thu, Apr 10, 2025 at 9:41 AM
To: [REDACTED]@ec.europa.eu" <[REDACTED]@ec.europa.eu>

Dear Sir, Dear Madam,

I hope this message finds you well.

*This is a kind reminder regarding your participation in the upcoming **DSA Multi-stakeholder workshop on Systemic Risks** scheduled for **7 May 2025, 9:00-18:30 CET in Brussels**.*

*We kindly request that you confirm your attendance by **registering via this [form](#)** . Your prompt response will be greatly appreciated.*

Should you require any additional information or have any specific inquiries, please do not hesitate to contact us.

Thank you for your attention, and we look forward to your participation.

*Kind regards,
The DSA Team*

Exhibit 5

DSA Multi-Stakeholder Workshop
Thank You and Commission
Read-Out (Company 1)

From: [REDACTED]
To: [REDACTED]
Subject: Fwd: Thank you for attending the DSA Multi-stakeholder Workshop on Systemic Risks
Date: Wednesday, July 2, 2025 4:54:24 PM

----- Forwarded message -----

From: [REDACTED] <[REDACTED]>
Date: Wed, Jul 2, 2025 at 1:40 PM
Subject: Fwd: Thank you for attending the DSA Multi-stakeholder Workshop on Systemic Risks
To: [REDACTED] <[REDACTED]>

Here is the high lev readout (not as detailed as ours).
Still looking for the list of participants

----- Forwarded message -----

From: [REDACTED] <[REDACTED]@ec.europa.eu>
[REDACTED] <[REDACTED]@ec.europa.eu>
Date: Thu, 15 May 2025 at 10:44
Subject: Thank you for attending the DSA Multi-stakeholder Workshop on Systemic Risks
To: [REDACTED] <[REDACTED]@ec.europa.eu> <[REDACTED]@ec.europa.eu>

Dear Participant,

We wanted to take a moment to express our gratitude for your participation in the DSA Multi-stakeholder Workshop on Systemic Risks, which took place on 7 May 2025.

Your valuable input and feedback are greatly appreciated. If you have any additional comments or suggestions, please do not hesitate to share them with us at [REDACTED] <[REDACTED]@ec.europa.eu>.

A high-level summary of the event is now available on the Commission's website: <https://digital-strategy.ec.europa.eu/en/news/commission-holds-workshop-platforms-and-civil-society-assessment-online-risks>. We hope that the discussions and exchanges that took place during the sessions will contribute to collaborations between stakeholders, in line with the spirit of Recital 90 DSA.

Once again, thank you for your participation and contribution to the workshop.

Best Regards,

The Organising Team

--



Exhibit 6

DSA Multi-Stakeholder Workshop
Thank You and Commission
Read-Out (Company 2)

[External] Thank you for attending the DSA Multi-stakeholder Workshop on Systemic Risks

1 message

[REDACTED]@ec.europa.eu <[REDACTED]@ec.europa.eu> Thu, May 15, 2025 at 9:44 AM
To: "[REDACTED]@ec.europa.eu" <[REDACTED]@ec.europa.eu>

Dear Participant,

We wanted to take a moment to express our gratitude for your participation in the DSA Multi-stakeholder Workshop on Systemic Risks, which took place on 7 May 2025.

Your valuable input and feedback are greatly appreciated. If you have any additional comments or suggestions, please do not hesitate to share them with us at [REDACTED]@ec.europa.eu.

A high-level summary of the event is now available on the Commission's website: <https://digital-strategy.ec.europa.eu/en/news/commission-holds-workshop-platforms-and-civil-society-assessment-online-risks>. We hope that the discussions and exchanges that took place during the sessions will contribute to collaborations between stakeholders, in line with the spirit of Recital 90 DSA.

Once again, thank you for your participation and contribution to the workshop.

Best Regards,

The Organising Team

Exhibit 7

DSA Multi-Stakeholder Workshop Privacy Statement



EUROPEAN COMMISSION

PROTECTION OF YOUR PERSONAL DATA

This privacy statement provides information about the processing and the protection of your personal data.

Processing operation: DSA Multi-stakeholder workshop on Systemic Risks

Data Controller: European Commission, *DG CNECT, F2*

Record reference: [REDACTED] on events and meetings

Table of Contents

- 1. Introduction**
- 2. Why and how do we process your personal data?**
- 3. On what legal ground(s) do we process your personal data?**
- 4. Which personal data do we collect and further process?**
- 5. How long do we keep your personal data?**
- 6. How do we protect and safeguard your personal data?**
- 7. Who has access to your personal data and to whom is it disclosed?**
- 8. What are your rights and how can you exercise them?**
- 9. Contact information**
- 10. Where to find more detailed information?**

1. Introduction

The European Commission is committed to protect your personal data and to respect your privacy. The Commission collects and further processes personal data pursuant to [Regulation \(EU\) 2018/1725](#) of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

This privacy statement explains the reason for the processing of your personal data in the context of **DSA Multi-stakeholder workshop on Systemic Risks**. It explains the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the European Data Protection Supervisor.

The information in relation to processing operation '**DSA Multi-stakeholder workshop on Systemic Risks**' undertaken by **DG CNECT, Unit F2 Digital Services** of the European Commission, is presented below.

2. Why and how do we process your personal data?

Purpose of the processing operation:

DG CNECT, Unit F2 Digital Services collects and further processes your personal data to provide you with information about the DSA Multi-stakeholder workshop on Systemic Risks (before, during and after), to process your registration in those events and to follow up after the event.

Your personal data will not be used for any automated decision-making including profiling.

3. On what legal ground(s) do we process your personal data?

The processing operations linked to the organisation, management, promotion and follow-up of the **DSA Multi-stakeholder workshop on Systemic Risks** are necessary for the management and functioning of the Commission, as mandated by the Treaties. Those provisions are Article 11 of the Treaty on European Union and Article 15 of the Treaty on the Functioning of the European Union. Consequently, those processing operations are lawful under Article 5(1)(a) of Regulation (EU) 2018/1725 (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body).

4. Which personal data do we collect and further process?

The following personal data will be processed:

- contact details (function/title, first name, last name, name of organisation, e-mail address,).
- nationality, passport or identity card number and its date of issue and expiry date may be collected, so that the data subjects may obtain access to the premises where the meeting/event is held.

5. How long do we keep your personal data?

The Data Controller only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing.

For each of the categories of personal data that is processed, please find below the retention details and the reference to the relevant record of processing:

- ☐ All personal data related to the organisation and management of the **DSA Multi-stakeholder workshop on Systemic Risks** will be deleted **five years** at the latest after the last action in relation to the roundtable discussions.
- ☐ Personal data shared with the Directorate-General for Human Resources and Security of the European Commission for the participants to gain access to Commission buildings is kept **for 6 months** after the termination of the link between the data subject and the Commission. More information is available in the Record of Processing DPR-EC-00655 (Commission Physical Access Control System (PACS)).

6. How do we protect and safeguard your personal data?

All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored either on the servers of the European Commission or of its contractors. All processing operations are carried out pursuant to [Commission Decision \(EU, Euratom\) 2017/46](#) of 10 January 2017 on the security of communication and information systems in the European Commission.

In order to protect your personal data, the Commission has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

7. Who has access to your personal data and to whom is it disclosed?

Access to your personal data is provided to the Commission staff in DG CNECT Directorate F Unit F2 responsible for carrying out this processing operation and to other authorised Commission staff according to the “need to know” principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

Cookies

Cookies are short text files stored on a user’s device (such as a computer, tablet or phone) by a website. Cookies are used for the technical functioning of a website (functional cookies) or for gathering statistics (analytical cookies).

The registration for the **DSA Multi-stakeholder workshop on Systemic Risks** takes place via Event-Works¹. The cookies employed by the Commission on the registrant’s device for that

¹ For more information on the processing of personal data via Event-Works, see DPR-EC-00297 “Participants registration for Commission conferences and events using Event-Works”

purpose will be covered by the cookie policy of the Commission, which is available here: https://ec.europa.eu/info/cookies_en.

Cookies are stored by Europa Analytics, the corporate service which measures the effectiveness and efficiency of the European Commission's websites on EUROPA. More information is available in the Record of Processing DPR-EC-00685 (Europa Analytics).

Enabling these cookies is not strictly necessary for the website to work but it will provide you with a better browsing experience. You can delete or block these cookies, but if you do that, some features of the meeting/event website may not work as intended.

The cookie-related information is not used to identify data subjects personally and the pattern data is fully under the Commission's control. These cookies are not used for any purpose other than those described here.

Should you wish to opt your personal data out of our anonymised, aggregated statistics, you can do so on our cookies page. In particular, you can control and/or delete those cookies as you wish.

International transfers

Please note that pursuant to Article 3(13) of Regulation (EU) 2018/1725 public authorities (e.g. Court of Auditors, EU Court of Justice) which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients. The further processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law.

8. What are your rights and how can you exercise them?

You have specific rights as a 'data subject' under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access, your personal data and to rectify them in case your personal data are inaccurate or incomplete. Where applicable, you have the right to erase your personal data, to restrict the processing of your personal data, to object to the processing, and the right to data portability.

You have the right to object to the processing of your personal data, which is lawfully carried out pursuant to Article 5(1)(a) of Regulation (EU) 2018/1725 on grounds relating to your particular situation.

In case of conflict, you can contact the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given under Heading 9 below.

Where you wish to exercise your rights in the context of one or several specific processing operations, please provide their description (i.e. their Record reference(s) as specified under Heading 10 below) in your request.

9. Contact information

- **The Data Controller:** If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact [REDACTED] [@ec.europa.eu](mailto:[REDACTED]@ec.europa.eu).
- **The Data Protection Officer (DPO) of the Commission:** You may contact the Data Protection Officer ([REDACTED] [@ec.europa.eu](mailto:[REDACTED]@ec.europa.eu)) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.
- **The European Data Protection Supervisor (EDPS):** You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor ([REDACTED] [@edps.europa.eu](mailto:[REDACTED]@edps.europa.eu)) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the data controller.

10. Where to find more detailed information?

The Commission Data Protection Officer (DPO) publishes the register of all processing operations on personal data by the European Commission, which have been documented and notified to him. You may access the register via the following link: <http://ec.europa.eu/dpo-register>.

Exhibit 8

Submission by Polish National Research
Institute to TikTok (Nov. 25, 2024)

creation_date	risk_id	intake_portal	country_name	reporting_team_agency
11/25/24 14:15			Poland	NASK

details

It has been suggested that electric cars are neither an ecological nor an economical solution.

clean_case_summary

Investigation Details EMEA Nov 25: Reported content: Sticker translation: Electric cars are the future? #business #mission #economy #politics #intelligence #europeanunion #poland #ukraine #greenddeal #ecology IM assessment: unable to confirm violation, no ASR available. Looped in PL PES for review EMEA Nov 26: No violation according to PES Enforcement Action Details N/A - No violation

reported_entity	final_action_taken	other_info
https://www.tiktok.com/@biznesmisja/video/7440473235617107222?_r=1&_t=8revginrPeQ	No Action	

Exhibit 9

Submission by French National Police
to X (June 11, 2023)

LRT Case ID	Status	Request Type	Filename	SC Case No.	Delivery	Format	Account Count	Requester Name
[REDACTED]	Closed	Content Removal Request	[REDACTED]	[REDACTED]	LEGOS	Formal Request	1	DCPJ PHAROS

Requester Email	Requester Country	Created At	Updated At	Production Date	Additional Filenames	Issue Reported	Emergency Disclosure	Info Requested	Linked Requests
[REDACTED] @interieur.gouv.fr	France	6/11/2023 5:21	6/11/2023 8:07		[REDACTED]	Violent Threat / Incitement, Illegal Content > Article 222-33-3 Al 2			

Accounts	Bounced Users	TOS Suspensions	Deactivated Users	Requester Type	Requester Title	Requester Office	Requester City	Requester State	Requester Phone
@EdBurke85403199	0	0	0	Government / Law Enforcement	OFFICIER DE POLICE JUDICIAIRE	National Police	NANTERRE		[REDACTED]

LEGOS Data**Created By**

LEGOS_Issue_Type: Violent threats or incitement;
LEGOS_Additional_Info: This is the video of the knife attack on children under the age of 3 in Annecy in France on 08/06/2023

Dissemination of images of an offence of wilful bodily harm
Article 222-33-3 Al 2

vidéo attaque couteau Annecy
art6;
LEGOS_Lumen_Notice_Acknowledgement: Yes;
LEGOS_Lumen_Notice_Redaction_Info: ;
LEGOS_Lumen_Notice_Prohibition_Reason: ;
LEGOS_Quick_Review: No;
LEGOS_Locale: French

intake_service

Exhibit 10

Submission by German authorities to
X (Dec. 9, 2024)

I. Sichtung

Az: [REDACTED]

<https://x.com/michaelboese191/status/1821603311356932268>

(3) Michael Böse auf X: „@focusonline Das ganze Pack abschieben!“ / X
<https://x.com/michaelboese191/status/1821603311356932268>

X

Startseite

Entdecken

Mitteilungen

Nachrichten

Grok


Lesezeichen

Communities


Premium

Verifizierte Organe

Post




FOCUS online @focusonline · 8. Aug.
Syrische Familie beging 110 Straftaten: Jetzt spricht der Vater und gibt Jugendamt die Schuld



Messerkiller von Stuttgart in U-Haft - Vater gibt Jugendamt die Schuld

Von focus.de






765 308 1.378 84.161




Michael Böse @michaelboese191

Das ganze Pack abschieben!

7:44 nachm. · 8. Aug. 2024 · 21 Mal angezeigt


    

 Deine Antwort posten


Antworten

Suchen

Relevante Personen

 **Michael Böse** @michaelboese191

Folgen

 **FOCUS online** @focusonline

Folgen

Impressum: bfurl.de/Impressum
Datenschutzerklärung: bfurl.de/Datenschutz

Was gibt's Neues?

Trend in Deutschland
Annalachen

Trend in Deutschland
#GrueneRausausallenParlamenten

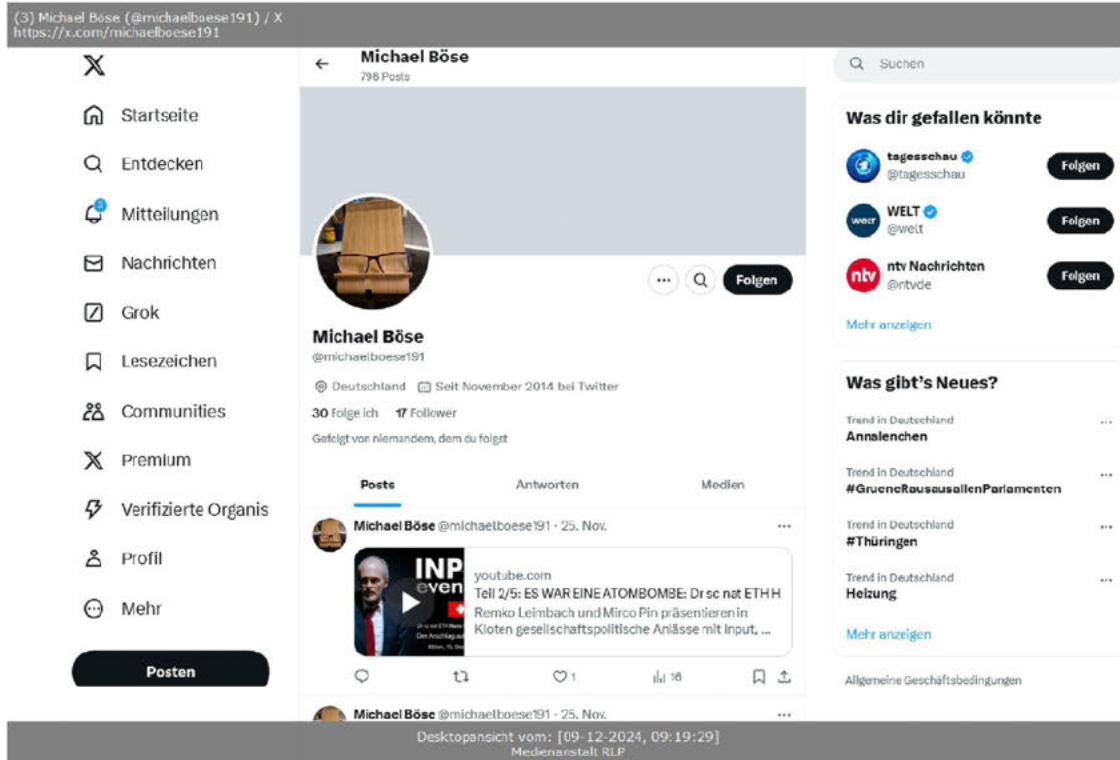
Trend in Deutschland
#Thüringen

Desktopansicht vom: [09-12-2024, 09:19:00]
Medienanstalt RLP

Profil: Michael Böse

90

Highly Confidential



Beschreibung:

Der Nutzer bezieht sich auf einen Focus-online-Bertrag vom 8. August, in dem von einer syrischen Familie berichtet wird, die 110 Straftaten begangen habe und der Vater gäbe dem Jugendamt die Schuld.

Der Nutzer kommentiert: „Das ganze Pack abschieben!“

Rechtliche Bewertung:

Nach hiesiger Bewertung könnte eine strafrechtliche Relevanz gem. § 130 I StGB (Aufstachelung zum Hass, Aufforderung zu Gewalt- und Willkürmaßnahmen oder Angriff der Menschenwürde) gegeben sein. Hier wird gegen eine nationale Gruppe (Syrier) zum Hass aufgestachelt und zu Gewalt- und Willkürmaßnahmen aufgefordert.

Nach § 4 (1) 3 JMStV könnte es sich um ein unzulässiges Angebot mit demselben Sachverhalt handeln: Der Autor stachelt zum Hass gegen Teile der Bevölkerung oder gegen eine nationale oder durch ihr Volkstum bestimmte Gruppe auf und greift die Menschenwürde der dieser Gruppe Angehörigen dadurch an, dass Teile der Bevölkerung oder diese Gruppe beschimpft, böswillig verächtlich gemacht oder verleumdet werden.

Description:

The user refers to a Focus online article from 8 August in which a Syrian family is reported to have committed 110 criminal offences and the father blames the youth welfare office.

The user comments: 'Deport the whole lot of them!' Legal Evaluation:

Legal Evaluation:

According to our evaluation here, this could be relevant under criminal law pursuant to Section 130 sentence 1 StGB, German Criminal Code (incitement to hatred, incitement to violence and arbitrary measures or attacks on human dignity). Here, hatred is incited against a national group (Syrians) and violence and arbitrary measures are called for.

According to Section 4 sentence (1) No. 3 JMStV, Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and Telemedia, this could be an unauthorised offer with the same content: The author incites hatred against parts of the population or against a national group or a group defined by its ethnicity, and attacks the human dignity of those belonging to this group by insulting, maliciously denigrating or defaming parts of the population or this group.

Ludwigshafen, 09.12.2024

pg

Exhibit 11

Emails between European Commission and
American Platform (Oct. 8, 2021)

Re: [REDACTED]'s state of consideration on the Code of Practice on Disinformation

Friday, October 8, 2021 at 7:19:52 PM Pacific Daylight Time

To: [REDACTED]@ec.europa.eu [REDACTED]@ec.europa.eu
Cc: [REDACTED] [REDACTED]

Hello, [REDACTED], thank you for being in touch and for the well wishes toward [REDACTED]. They are indeed in order, as I found out just this morning! A beautiful baby girl and mother and daughter are both doing wonderfully.

However, as you know, with [REDACTED] out and the small size of our team, our capacity considerations regarding the code unfortunately haven't changed, and we'll be unable to join in the current process. I do appreciate your keeping me in the loop, however, and sharing these updates.

Best wishes,

[REDACTED]

[REDACTED]



On Fri, Oct 8, 2021 at 9:06 AM [REDACTED]@ec.europa.eu <[REDACTED]@ec.europa.eu> wrote:

Dear [REDACTED],

We have not been in touch for a while, so we just wanted to check in whether there are any news with regards to [REDACTED]'s considerations on joining the Code of Practice?

To keep you in the loop, we take the opportunity to quickly update you on where the Code's drafting process stands. After the last Assembly meeting, the prospective and current signatories of the Code has started to proceed quickly with the work on the text of the actual Code, and this week they started to switch from the preamble of the document to the part related to integrity of services.

The Commission has also published a press release providing information on where the process stands: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_4945

In any case, should you have any further questions or would like to schedule an additional meeting, please do not hesitate to come back to us.

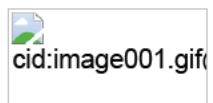
We hope this email finds you well, please also extend our warm congratulations to [REDACTED] of course if those are already in order!

Have a nice weekend,

Kind Regards,

[REDACTED]

[REDACTED]
Directorate I – Media Policy



European Commission
Communications Networks, Content & Technology (DG CNECT)

[REDACTED]
B-1160 Brussels/Belgium

Tel: [REDACTED]

[REDACTED] [@ec.europa.eu](mailto:[REDACTED]@ec.europa.eu)

Attachments:

image001.gif 3.8k

Exhibit 12

Emails between European Commission and
American Platform (Sept. 2021)

Re: Information meeting for interested new signatories to the 2021 EU Code of Practice on Disinformation

1 message

Mon, Sep 13, 2021 at 8:00 AM

To: [REDACTED] <[REDACTED]@ec.europa.eu>
Cc: [REDACTED] <[REDACTED]@ec.europa.eu>

Thank you for this invitation. Unfortunately, we will be unable to attend the meeting.

Kind regards,

[REDACTED]



On Thu, Sep 9, 2021 at 3:59 AM [REDACTED] <[REDACTED]@ec.europa.eu> wrote:

Dear Stakeholder,

Thank you once again for your interest in joining the Code of Practice on Disinformation.

We would like to invite you to an information meeting organised for potential new signatories. The meeting will assemble current signatories, new signatories that have already submitted an application as well as organisations that are considering to submit one.

The purpose of the meeting is to connect potential new signatories with the current signatories and giving you an opportunity to briefly present your services as well as the type of commitments that you are considering to take. The signatories will also provide further information regarding the drafting process foreseen for the revision of the Code.

The meeting will take place online on **Wednesday 15 September 2021 16:00 - 18:30**. Please find attached the agenda.

We would appreciate if you could confirm **by 13 September** your organisation's participation in the meeting, including the name of the representative(s) joining. We would suggest a maximum of two representatives per organisation. The WebEx invitation will follow in a separate email.

Should you have any questions regarding the meeting, please don't hesitate to reach out to us.

Kind regards,

[REDACTED]
Head of Unit



European Commission
DG Communications Networks, Content and Technology
Unit I4 – Media convergence and Social Media
B-1049 Brussels/Belgium

Exhibit 13

Emails between European Commission and
American Platform (Aug. 2021)

RE: Strengthened Code of Practice on Disinformation - Call for interest

1 message

To: [REDACTED] <[REDACTED]@ec.europa.eu> Thu, Aug 19, 2021 at 5:27 AM
Cc: [REDACTED] <[REDACTED]@ec.europa.eu>, [REDACTED] <[REDACTED]@ec.europa.eu>, [REDACTED] <[REDACTED]@ec.europa.eu>

Dear [REDACTED],

Thank you very much for the invite,

Talk to you on Monday!

Best,

[REDACTED]

From: [REDACTED] <[REDACTED]>
Sent: Thursday, August 19, 2021 12:35 PM
To: [REDACTED] (CNECT) <[REDACTED]@ec.europa.eu>
Cc: [REDACTED] <[REDACTED]@ec.europa.eu>, [REDACTED] (CNECT) <[REDACTED]@ec.europa.eu>, [REDACTED] <[REDACTED]@ec.europa.eu>
Subject: Re: Strengthened Code of Practice on Disinformation - Call for interest

Dear [REDACTED],

Perfect, I sent an invite for Monday. Looking forward to our chat.

Kind regards,

[REDACTED]

From: [REDACTED] <[REDACTED]@ec.europa.eu>
Date: Wednesday, 18 August 2021 at 16:12
To: [REDACTED] <[REDACTED]>
Cc: [REDACTED] <[REDACTED]@ec.europa.eu>, [REDACTED] <[REDACTED]@ec.europa.eu>, [REDACTED] <[REDACTED]@ec.europa.eu>, [REDACTED] <[REDACTED]@ec.europa.eu>
Subject: RE: Strengthened Code of Practice on Disinformation - Call for interest

Dear [REDACTED],

Thanks a lot! I'd say let's meet on Monday 23, 1730.

On our side, [REDACTED], [REDACTED] and I will participate.

Thank you already for sending the invite.

Looking forward to meeting you,

Regards,

[REDACTED]

From: [REDACTED] <[REDACTED]>
Sent: Wednesday, August 18, 2021 3:44 PM

To: [REDACTED] (CNECT) <[REDACTED]@ec.europa.eu>
Cc: [REDACTED] <[REDACTED]@ec.europa.eu>; [REDACTED] (CNECT) <[REDACTED]@ec.europa.eu>; [REDACTED] <[REDACTED]@ec.europa.eu>
Subject: Re: Strengthened Code of Practice on Disinformation - Call for interest

Hello [REDACTED],

We could offer either:

- Monday 23rd Aug, at 17.30
- Friday 27th Aug, at 18.00

The discussion could probably last 30-45 mins.

Let us know what you prefer and I'll send you an invite.

Best,

[REDACTED]

From: [REDACTED] <[REDACTED]@ec.europa.eu>
Date: Friday, 13 August 2021 at 20:59
To: [REDACTED] <[REDACTED]@ec.europa.eu>
Cc: [REDACTED] <[REDACTED]@ec.europa.eu>; [REDACTED] <[REDACTED]@ec.europa.eu>; [REDACTED] <[REDACTED]@ec.europa.eu>; [REDACTED] <[REDACTED]@ec.europa.eu>
Subject: RE: Strengthened Code of Practice on Disinformation - Call for interest

Dear [REDACTED],

Thank you for your email. We are very happy to arrange a meeting after 17h to allow [REDACTED] to join.

Next week, Monday, Wednesday and Friday would easily work, while the week after besides Wednesday, we are available most days.

Have a great weekend,

Best,

[REDACTED]

[REDACTED]
Policy Officer

European Commission
DG Communications Networks, Content and Technology
Unit I4 – Media convergence and Social Media
[REDACTED]
B-1049 Brussels/Belgium
[REDACTED]@ec.europa.eu
<https://ec.europa.eu/digital-single-market>

From: [REDACTED] <[REDACTED]>
Sent: Friday, August 13, 2021 5:04 PM
To: [REDACTED] (CNECT) <[REDACTED]@ec.europa.eu>
Cc: [REDACTED] <[REDACTED]@ec.europa.eu>; [REDACTED] (CNECT) <[REDACTED]@ec.europa.eu>; [REDACTED]
Subject: FW: Strengthened Code of Practice on Disinformation - Call for interest

Dear [REDACTED],

Thanks for getting back to us. We would be happy to discuss this matter over the following weeks.

Could you please provide us with some suggested slots on your side? If possible, they should be after 17.00 to allow my colleague [REDACTED] to join as well.

Looking forward to hearing from you.

Kind regards,

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

----- Forwarded message -----

From: [REDACTED] <[REDACTED]@ec.europa.eu>

Date: Thu, Jul 15, 2021 at 5:45 AM

Subject: Strengthened Code of Practice on Disinformation - Call for interest

To: [REDACTED] <[REDACTED]>

CC: [REDACTED] <[REDACTED]@ec.europa.eu>, [REDACTED] <[REDACTED]@ec.europa.eu> [REDACTED] <[REDACTED]@ec.europa.eu>

Dear [REDACTED],

Hope this email finds you well. I am contacting you back after the exchanges we had back February, to let you know the further steps we have taken with regards to the Code of Practice on Disinformation, as we promised to do after our meeting back then.

On 26 May 2021, we published a document of Guidance to strengthen the Code of Practice on Disinformation (https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2585) and make it an even more effective tool for countering disinformation online.

One of the main aims of the strengthened Code is to broaden the participation and achieve a more comprehensive and coordinated response to the spread of disinformation across all relevant actors of the online ecosystem. Both the current signatories and the Commission would like to see included in the new Code **more players, signing up to tailored commitments relevant for the services that they provide**, in order to match the diversity of services of a wider array of signatories.

Last week, we published with the current signatories of the Code a **joint call for interest for new signatories** (<https://digital-strategy.ec.europa.eu/en/joint-call-interest-join-code-practice-disinformation>, see also text attached). New signatories would have the possibility to participate actively in the preparation of the strengthened Code and co-shape the commitments that are relevant to them.

The current signatories have just kicked off the review process and are expected to adopt the revised Code by the end of the year.

It would be ideal if we could have a chat sometime before September to explore in what way we could possibly have [REDACTED] involved in this process at some stage.

Please let me know your thoughts and some possible timing for a discussion. As I will be on leave starting Monday, you can see my colleague [REDACTED] in copy should you want to reach out to him before the end of July – also the dedicated email for the Code of Practice is an easy way to reach our team.

Thanking you in advance for your availability,

Kind regards,

[REDACTED]

[REDACTED]
Policy Officer



European Commission
DG Communications Networks, Content and Technology
Unit I4 – Media convergence and Social Media
[REDACTED]
B-1049 Brussels/Belgium

[REDACTED]

[REDACTED]@ec.europa.eu
<https://ec.europa.eu/digital-single-market>

--

[REDACTED]

--

[REDACTED]

Exhibit 14

Emails between European Commission and
American Platform (Feb. 2021)

RE: Contacts - Code of Practice on disinformation

1 message

To: [REDACTED] <[REDACTED]@ec.europa.eu>
Cc: [REDACTED] <[REDACTED]@ec.europa.eu>

Tue, Feb 9, 2021 at 11:23 AM

Dear [REDACTED],

Thank you very much for your availability. We are indeed available for a quick chat on Friday, 16:30 Brussels time.

I will follow tomorrow with the meeting details.

Best,

[REDACTED]

From: [REDACTED] <[REDACTED]>
Sent: Monday, February 8, 2021 11:56 PM
To: [REDACTED] (CNECT) <[REDACTED]@ec.europa.eu>
Cc: [REDACTED] (CNECT) <[REDACTED]@ec.europa.eu>
Subject: Re: Contacts - Code of Practice on disinformation

Hi [REDACTED], thanks for following up on this. Would you be free for a quick video chat later this week to discuss further? I could do 16:30 Brussels time on Wednesday, Thursday, or Friday of this week, if any of those times work for you.

Kind regards,

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

 [REDACTED]

This email may be confidential or privileged. If you received this communication by mistake, please don't forward it to anyone else, erase all copies and attachments, and notify the sender.

On Mon, Feb 8, 2021 at 12:33 PM [REDACTED] <[REDACTED]@ec.europa.eu> wrote:

Dear [REDACTED],

Thank you again for answering my quick message on LinkedIn.

As briefly mentioned, I am part of the European Commission's team that works on the implementation of the Code of Practice on Disinformation - see <https://ec.europa.eu/digital-single-market/en/code-practice-disinformation>. The Code has been signed by the main online platforms (Facebook, Google, Twitter, Microsoft and TikTok) and relevant players in the advertising sector, and contains commitments to take measures to limit the spread of disinformation online.

We are working to strengthen the Code in accordance to the latest EU legislative proposals, and will be releasing some Guidance on how to proceed further. Hence, as [REDACTED] has become the more and more a relevant player in the European market, we wanted to reach out to propose that [REDACTED] takes part in the process.

I will be following this up with a formal email, but I take this chance to share my contacts with you and to thank you in advance for your availability.

Do not hesitate to come back to me should you require further clarifications.

My Best Regards,

[Redacted]

[Redacted]
Policy Officer



European Commission
DG Communications Networks, Content and Technology
Unit for Media Convergence and Social Media

[Redacted]
B-1049 Brussels/Belgium

[Redacted] [@ec.europa.eu](mailto:[Redacted]@ec.europa.eu)
<https://ec.europa.eu/digital-single-market>

Exhibit 15

Eva Glawischnig-Piesczek v. Facebook
Ireland Ltd., 2019 E.C.R.

JUDGMENT OF THE COURT (Third Chamber)

3 October 2019 (*)

(Reference for a preliminary ruling — Information society — Free movement of services — Directive 2000/31/EC — Liability of intermediary service providers — Article 14(1) and (3) — Hosting services provider — Possibility of requiring the service provider to terminate or prevent an infringement — Article 18(1) — Personal, material and territorial limits on the scope of an injunction — Article 15(1) — No general obligation to monitor)

In Case C-18/18,

REQUEST for a preliminary ruling under Article 267 TFEU from the Oberster Gerichtshof (Supreme Court, Austria), made by decision of 25 October 2017, received at the Court on 10 January 2018, in the proceedings

Eva Glawischnig-Piesczek

v

Facebook Ireland Limited,

THE COURT (Third Chamber),

composed of A. Prechal, President of the Chamber, F. Biltgen, J. Malenovský (Rapporteur), C.G. Fernlund and L.S. Rossi, Judges,

Advocate General: M. Szpunar,

Registrar: D. Dittert, Head of Unit,

having regard to the written procedure and further to the hearing on 13 February 2019,

after considering the observations submitted on behalf of:

- Ms Glawischnig-Piesczek, by M. Windhager and W. Niklfeld, Rechtsanwälte,
- Facebook Ireland Limited, by G. Kresbach, K. Struckmann and A. Tauchen, Rechtsanwälte,
- the Austrian Government, by G. Hesse, G. Kunnert and A. Jurgutyte-Ruez, acting as Agents,
- the Latvian Government, by I. Kucina, E. Petrocka-Petrovska and V. Soņeca, acting as Agents,
- the Portuguese Government, by L. Inez Fernandes and M. Figueiredo, acting as Agents, and T. Rendas, Legal Adviser.
- the Finnish Government, by J. Heliskoski, acting as Agent,
- the European Commission, by G. Braun, F. Wilman, S.L. Kalèda, and P. Costa de Oliveira, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 4 June 2019,

gives the following

Judgment

- 1 This request for a preliminary ruling concerns the interpretation of Article 15(1) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ('Directive on electronic commerce') (OJ 2000 L 178, p. 1).
- 2 The request has been made in proceedings between Ms Eva Glawischnig-Piesczek and Facebook Ireland Limited whose registered address is in Ireland, concerning the publication on the page of a hosted user on the social network Facebook of a message containing statements harmful to the reputation of Ms Glawischnig-Piesczek.

Legal context

EU law

- 3 Recitals 6, 7, 9, 10, 40, 41, 45 to 48, 52, 58 and 60 of Directive 2000/31 state:
 - '(6) ... by dealing only with certain specific matters which give rise to problems for the internal market, this Directive is fully consistent with the need to respect the principle of subsidiarity as set out in Article 5 of the Treaty.
 - (7) In order to ensure legal certainty and consumer confidence, this Directive must lay down a clear and general framework to cover certain legal aspects of electronic commerce in the internal market.
 - ...
 - (9) The free movement of information society services can in many cases be a specific reflection in Community law of a more general principle, namely freedom of expression as enshrined in Article 10(1) of the [European] Convention for the Protection of Human Rights and Fundamental Freedoms, [signed in Rome on 4 November 1950,] which has been ratified by all the Member States; for this reason, directives covering the supply of information society services must ensure that this activity may be engaged in freely in the light of that Article, subject only to the restrictions laid down in paragraph 2 of that Article and in Article 46(1) of the Treaty; this Directive is not intended to affect national fundamental rules and principles relating to freedom of expression.
 - (10) In accordance with the principle of proportionality, the measures provided for in this Directive are strictly limited to the minimum needed to achieve the objective of the proper functioning of the internal market; where action at Community level is necessary, and in order to guarantee an area which is truly without internal frontiers as far as electronic commerce is concerned, the Directive must ensure a high level of protection of objectives of general interest, in particular the protection of minors and human dignity, consumer protection and the protection of public health; ...
 - ...
 - (40) Both existing and emerging disparities in Member States' legislation and case-law concerning liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition; service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities; this Directive should constitute the appropriate basis

for the development of rapid and reliable procedures for removing and disabling access to illegal information; ...

- (41) This Directive strikes a balance between the different interests at stake and establishes principles upon which industry agreements and standards can be based.

...

- (45) The limitations of the liability of intermediary service providers established in this directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.

- (46) In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level; this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.

- (47) Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation.

- (48) This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.

...

- (52) The effective exercise of the freedoms of the internal market makes it necessary to guarantee victims effective access to means of settling disputes; damage which may arise in connection with information society services is characterised both by its rapidity and by its geographical extent; in view of this specific character and the need to ensure that national authorities do not endanger the mutual confidence which they should have in one another, this Directive requests Member States to ensure that appropriate court actions are available; Member States should examine the need to provide access to judicial procedures by appropriate electronic means.

...

- (58) This Directive should not apply to services supplied by service providers established in a third country; in view of the global dimension of electronic commerce, it is, however, appropriate to ensure that the Community rules are consistent with international rules; this Directive is without prejudice to the results of discussions within international organisations (amongst others WTO, OECD, Uncitral) on legal issues.

...

- (60) In order to allow the unhampered development of electronic commerce, the legal framework must be clear and simple, predictable and consistent with the rules applicable at international level so that it does not adversely affect the competitiveness of European industry or impede innovation in that sector.'

4 Article 14 of Directive 2000/31, entitled ‘Hosting’, states:

‘1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent;

or

(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

...

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States’ legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.’

5 Article 15(1) of that directive provides:

‘Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.’

6 Article 18(1) of that directive provides:

‘Member States shall ensure that court actions available under national law concerning information society services’ activities allow for the rapid adoption of measures, including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.’

Austrian law

7 In accordance with Paragraph 1330(1) of the Allgemeines Bürgerliches Gesetzbuch (General Civil Code), anyone who has sustained actual harm or loss of profit owing to damage to his reputation is entitled to claim compensation. Under subparagraph 2 of that paragraph, the same is to apply when a person reports facts prejudicial to the reputation, material situation and future prospects of a third party which he knew or ought to have known to be inaccurate. In that case, a denial and publication of that denial may be required.

8 According to Paragraph 78(1) of the Urheberrechtsgesetz (Law on copyright), images representing a person must not be displayed publicly or disseminated in another way that makes them accessible to the public if such publication or dissemination harms the legitimate interests of the person concerned or, where that person has deceased without having authorised or ordered such publication, the legitimate interests of a close relative.

9 Under Paragraph 18(1) of the E-Commerce-Gesetz (Law on electronic commerce), hosting services providers are under no general obligation to monitor the information which they store, transmit or make available, or actively to seek facts or circumstances indicating illegal activity.

The dispute in the main proceedings and the questions referred for a preliminary ruling

- 10 Ms Eva Glawischnig-Piesczek was a member of the Nationalrat (National Council, Austria), chair of the parliamentary party 'die Grünen' (The Greens) and federal spokesperson for that party.
- 11 Facebook Ireland operates a global social media platform ('Facebook Service') for users located outside the United States of America and Canada.
- 12 On 3 April 2016, a Facebook Service user shared on that user's personal page an article from the Austrian online news magazine *oe24.at* entitled 'Greens: Minimum income for refugees should stay', which had the effect of generating on that page a 'thumbnail' of the original site, containing the title and a brief summary of the article, and a photograph of Ms Glawischnig-Piesczek. That user also published, in connection with that article, a comment which the referring court found to be harmful to the reputation of the applicant in the main proceedings, and which insulted and defamed her. This post could be accessed by any Facebook user.
- 13 By letter of 7 July 2016, Ms Glawischnig-Piesczek, inter alia, asked Facebook Ireland to delete that comment.
- 14 Because Facebook Ireland did not withdraw the comment in question, Ms Glawischnig-Piesczek brought an action before the Handelsgericht Wien (Commercial Court, Vienna, Austria) which, by interim order of 7 December 2016, directed Facebook Ireland, with immediate effect and until the proceedings relating to the action for a prohibitory injunction have been finally concluded, to cease and desist from publishing and/or disseminating photographs showing the applicant [in the main proceedings] if the accompanying text contained the assertions, verbatim and/or using words having an equivalent meaning as that of the comment referred to in paragraph 12 above.
- 15 Facebook Ireland disabled access in Austria to the content initially published.
- 16 On appeal, the Oberlandesgericht Wien (Higher Regional Court, Vienna, Austria) upheld the order made at first instance as regards the identical allegations. However, it also held that the dissemination of allegations of equivalent content had to cease only as regards those brought to the knowledge of Facebook Ireland by the applicant in the main proceedings, by third parties or otherwise.
- 17 The Handelsgericht Wien (Commercial Court, Vienna) and the Oberlandesgericht Wien (Higher Regional Court, Vienna) based their decisions on Paragraph 78 of the Law on copyright and Paragraph 1330 of the General Civil Code, on the ground, inter alia, that the published comment contained statements which were excessively harmful to the reputation of Ms Glawischnig-Piesczek and, in addition, gave the impression that she was involved in unlawful conduct, without providing the slightest evidence in that regard.
- 18 Each of the parties in the main proceedings lodged appeals on a point of law at the Oberster Gerichtshof (Supreme Court, Austria).
- 19 Having been called on to adjudicate whether the cease and desist order made against a host provider which operates a social network with a large number of users may also be extended to statements with identical wording and/or having equivalent content of which it is not aware, the Oberster Gerichtshof (Supreme Court) states that, in accordance with its own case-law, such an obligation must be considered to be proportionate where the host provider was already aware that the interests of the person concerned had been harmed on at least one occasion as a result of a user's post and the risk that other infringements may be committed is thus demonstrated.
- 20 However, considering that the dispute before it raises questions of the interpretation of EU law, the Oberster Gerichtshof (Supreme Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:
- '(1) Does Article 15(1) of Directive [2000/31] generally preclude any of the obligations listed below of a host provider which has not expeditiously removed illegal information, specifically not just this

illegal information within the meaning of Article 14(1)(a) of [that] directive, but also other identically worded items of information:

- worldwide;
 - in the relevant Member State;
 - of the relevant user worldwide;
 - of the relevant user in the relevant Member State?
- (2) In so far as Question 1 is answered in the negative: does this also apply in each case for information with an equivalent meaning?
- (3) Does this also apply for information with an equivalent meaning as soon as the operator has become aware of this circumstance?’

Consideration of the questions referred

The first and second questions

- 21 By its first and second questions, which it is appropriate to examine together, the referring court asks, in essence, whether Directive 2000/31, in particular Article 15(1), must be interpreted as meaning that it precludes a court of a Member State from:
- ordering a host provider to remove information which it stores, the content of which is identical to the content of information which was previously declared to be illegal, or to block access to that information, irrespective of who requested the storage of that information;
 - ordering a host provider to remove information which it stores, the content of which is equivalent to the content of information which was previously declared to be illegal, or to block access to that information, and
 - extending the effects of that injunction worldwide.
- 22 As a preliminary point, it is common ground that Facebook Ireland provides the services of a host provider for the purposes of Article 14 of Directive 2000/31.
- 23 In that respect, it should be recalled that Article 14(1) of that directive is intended to exempt the host provider from liability where it satisfies one of the two conditions listed in that provision, that is to say, not having knowledge of the illegal activity or information, or acting expeditiously to remove or to disable access to that information as soon as it becomes aware of it.
- 24 In addition, it is apparent from Article 14(3) of Directive 2000/31, read in conjunction with recital 45, that that exemption is without prejudice to the power of the national courts or administrative authorities to require the host provider concerned to terminate or prevent an infringement, including by removing the illegal information or by disabling access to it.
- 25 It follows that, as the Advocate General stated in point 32 of his Opinion, a host provider may be the addressee of injunctions adopted on the basis of the national law of a Member State, even if it satisfies one of the alternate conditions set out in Article 14(1) of Directive 2000/31, that is to say, even in the event that it is not considered to be liable.
- 26 Furthermore, Article 18 of Directive 2000/31, which is part of Chapter III of that directive entitled ‘Implementation’, provides in paragraph 1 that Member States must ensure that court actions available

under national law concerning information society services' activities allow for the rapid adoption of measures, including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.

- 27 In the present case, as follows from paragraph 13 above and from the actual wording of the questions raised, Facebook Ireland, first of all, did have knowledge of the illegal information at issue. Next, that company did not act expeditiously to remove or to disable access to that information, as laid down in Article 14(1) of Directive 2000/31. In the end, the applicant in the main proceedings brought an action before a national court for an injunction like the one referred to in Article 18.
- 28 Recital 52 of that directive states that the specific character arising from the fact that the damage which may arise in connection with information society services is characterised both by its rapidity and by its geographical extent, and also by the need to ensure that national authorities do not endanger the mutual confidence which they should have in one another, led the legislature of the European Union to request Member States to ensure that appropriate court actions are available.
- 29 Thus, when implementing Article 18(1) of Directive 2000/31, Member States have a particularly broad discretion in relation to the actions and procedures for taking the necessary measures.
- 30 Moreover, given that those measures, according to a number of linguistic versions of that provision, including the English, Spanish and French-language versions, are expressly intended to terminate 'any' alleged infringement and to prevent 'any' further impairment of the interests involved, no limitation on their scope can, in principle, be presumed for the purposes of their implementation. That interpretation is not called into question by the fact that other linguistic versions of that provision, including the German version, provide that those measures are intended to terminate 'an alleged infringement' and to prevent 'further impairment of the interests involved'.
- 31 Article 15(1) of Directive 2000/31 states that Member States must not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, or a general obligation actively to seek facts or circumstances indicating illegal activity.
- 32 It is by taking all of those provisions into consideration that the Court will reply to the questions raised by the referring court.
- 33 In the first place, the referring court asks, in essence, whether Article 15(1) of Directive 2000/31 precludes a court of a Member State from ordering a host provider to remove or block access to information which it stores, the content of which is identical to the content of information which was previously declared to be illegal.
- 34 In that regard, although Article 15(1) prohibits Member States from imposing on host providers a general obligation to monitor information which they transmit or store, or a general obligation actively to seek facts or circumstances indicating illegal activity, as is clear from recital 47 of that directive, such a prohibition does not concern the monitoring obligations 'in a specific case'.
- 35 Such a specific case may, in particular, be found, as in the main proceedings, in a particular piece of information stored by the host provider concerned at the request of a certain user of its social network, the content of which was examined and assessed by a court having jurisdiction in the Member State, which, following its assessment, declared it to be illegal.
- 36 Given that a social network facilitates the swift flow of information stored by the host provider between its different users, there is a genuine risk that information which was held to be illegal is subsequently reproduced and shared by another user of that network.

- 37 In those circumstances, in order to ensure that the host provider at issue prevents any further impairment of the interests involved, it is legitimate for the court having jurisdiction to be able to require that host provider to block access to the information stored, the content of which is identical to the content previously declared to be illegal, or to remove that information, irrespective of who requested the storage of that information. In particular, in view of the identical content of the information concerned, the injunction granted for that purpose cannot be regarded as imposing on the host provider an obligation to monitor generally the information which it stores, or a general obligation actively to seek facts or circumstances indicating illegal activity, as provided for in Article 15(1) of Directive 2000/31.
- 38 In the second place, the referring court asks, in essence, whether Article 15(1) of Directive 2000/31 precludes a court of a Member State from ordering a host provider to remove information which it stores, the content of which is equivalent to the content of information which was previously declared to be illegal, or to block access to that information.
- 39 It is apparent from the information set out in the order for reference that, in using the words ‘information with an equivalent meaning’, the referring court intends to refer to information conveying a message the content of which remains essentially unchanged and therefore diverges very little from the content which gave rise to the finding of illegality.
- 40 In that regard, it should be made clear that the illegality of the content of information does not in itself stem from the use of certain terms combined in a certain way, but from the fact that the message conveyed by that content is held to be illegal, when, as in the present case, it concerns defamatory statements made against a specific person.
- 41 It follows therefore that, in order for an injunction which is intended to bring an end to an illegal act and to prevent it being repeated, in addition to any further impairment of the interests involved, to be capable of achieving those objectives effectively, that injunction must be able to extend to information, the content of which, whilst essentially conveying the same message, is worded slightly differently, because of the words used or their combination, compared with the information whose content was declared to be illegal. Otherwise, as the referring court made clear, the effects of such an injunction could easily be circumvented by the storing of messages which are scarcely different from those which were previously declared to be illegal, which could result in the person concerned having to initiate multiple proceedings in order to bring an end to the conduct of which he is a victim.
- 42 However, it must also be observed that, in this context, as is apparent from Article 15(1) of Directive 2000/31 and as was observed in paragraph 34 above, a court of a Member State may not, first, grant an injunction against a host provider requiring it to monitor generally the information which it stores or, second, require that host provider actively to seek facts or circumstances underlying the illegal content.
- 43 In that regard, it should be pointed out in particular that, as is apparent from recital 41 of Directive 2000/31, in adopting that directive, the EU legislature wished to strike a balance between the different interests at stake.
- 44 Thus, Article 15(1) of Directive 2000/31 implies that the objective of an injunction such as the one referred to in Article 18(1) of that directive, read in conjunction with recital 41, consisting, inter alia, of effectively protecting a person’s reputation and honour, may not be pursued by imposing an excessive obligation on the host provider.
- 45 In light of the foregoing, it is important that the equivalent information referred to in paragraph 41 above contains specific elements which are properly identified in the injunction, such as the name of the person concerned by the infringement determined previously, the circumstances in which that infringement was determined and equivalent content to that which was declared to be illegal. Differences in the wording of that equivalent content, compared with the content which was declared to be illegal, must not, in any event, be such as to require the host provider concerned to carry out an independent assessment of that content.

- 46 In those circumstances, an obligation such as the one described in paragraphs 41 and 45 above, on the one hand — in so far as it also extends to information with equivalent content — appears to be sufficiently effective for ensuring that the person targeted by the defamatory statements is protected. On the other hand, that protection is not provided by means of an excessive obligation being imposed on the host provider, in so far as the monitoring of and search for information which it requires are limited to information containing the elements specified in the injunction, and its defamatory content of an equivalent nature does not require the host provider to carry out an independent assessment, since the latter has recourse to automated search tools and technologies.
- 47 Thus, such an injunction specifically does not impose on the host provider an obligation to monitor generally the information which it stores, or a general obligation actively to seek facts or circumstances indicating illegal activity, as provided for in Article 15(1) of Directive 2000/31.
- 48 In the third place, although the referring court does not provide any explanations in that regard in the grounds for its order for reference, the wording of the questions which it addressed to the Court suggests that its doubts also concern the issue whether Article 15(1) of Directive 2000/31 precludes injunctions such as those referred to in paragraphs 37 and 46 above from being able to produce effects which extend worldwide.
- 49 In order to answer that question, it must be observed that, as is apparent, notably from Article 18(1), Directive 2000/31 does not make provision in that regard for any limitation, including a territorial limitation, on the scope of the measures which Member States are entitled to adopt in accordance with that directive.
- 50 Consequently, and also with reference to paragraphs 29 and 30 above, Directive 2000/31 does not preclude those injunction measures from producing effects worldwide.
- 51 However, it is apparent from recitals 58 and 60 of that directive that, in view of the global dimension of electronic commerce, the EU legislature considered it necessary to ensure that EU rules in that area are consistent with the rules applicable at international level.
- 52 It is up to Member States to ensure that the measures which they adopt and which produce effects worldwide take due account of those rules.
- 53 In the light of all the foregoing, the answer to the first and second questions is that Directive 2000/31, in particular Article 15(1), must be interpreted as meaning that it does not preclude a court of a Member State from:
- ordering a host provider to remove information which it stores, the content of which is identical to the content of information which was previously declared to be unlawful, or to block access to that information, irrespective of who requested the storage of that information;
 - ordering a host provider to remove information which it stores, the content of which is equivalent to the content of information which was previously declared to be unlawful, or to block access to that information, provided that the monitoring of and search for the information concerned by such an injunction are limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the injunction, and provided that the differences in the wording of that equivalent content, compared with the wording characterising the information which was previously declared to be illegal, are not such as to require the host provider to carry out an independent assessment of that content, or
 - ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law.

The third question

- 54 In the light of the reply given to the first and second questions, it is not necessary to consider the third question referred.

Costs

- 55 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Third Chamber) hereby rules:

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), in particular Article 15(1), must be interpreted as meaning that it does not preclude a court of a Member State from:

- **ordering a host provider to remove information which it stores, the content of which is identical to the content of information which was previously declared to be unlawful, or to block access to that information, irrespective of who requested the storage of that information;**
- **ordering a host provider to remove information which it stores, the content of which is equivalent to the content of information which was previously declared to be unlawful, or to block access to that information, provided that the monitoring of and search for the information concerned by such an injunction are limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the injunction, and provided that the differences in the wording of that equivalent content, compared with the wording characterising the information which was previously declared to be illegal, are not such as to require the host provider to carry out an independent assessment of that content, and**
- **ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law.**

[Signatures]

* Language of the case: German.

Exhibit 16

Letter from Mr. Thierry Breton, Comm'r for Internal Market, European Comm'n, to Mr. Elon Musk, Owner, X Corp. (Aug. 12, 2024).



EUROPEAN COMMISSION

Thierry Breton
Member of the Commission

Brussels, 12 August 2024

Dear Mr Musk,

I am writing to you in the context of recent events in the United Kingdom and in relation to the planned broadcast on your platform X of a live conversation between a US presidential candidate and yourself, which will also be accessible to users in the EU.

I understand that you are currently doing a stress test of the platform. In this context, I am compelled to remind you of the due diligence obligations set out in the Digital Services Act (DSA), as outlined in my previous letter. As the individual entity ultimately controlling a platform with over 300 million users worldwide, of which one third in the EU, that has been designated as a Very Large Online Platform, you have the legal obligation to ensure X's compliance with EU law and in particular the DSA in the EU.

This notably means ensuring, on one hand, that freedom of expression and of information, including media freedom and pluralism, are effectively protected and, on the other hand, that all proportionate and effective mitigation measures are put in place regarding the amplification of harmful content in connection with relevant events, including live streaming, which, if unaddressed, might increase the risk profile of X and generate detrimental effects on civic discourse and public security. This is important against the background of recent examples of public unrest brought about by the amplification of content that promotes hatred, disorder, incitement to violence, or certain instances of disinformation.

It also implies i) informing EU judicial and administrative authorities without undue delay on the measures taken to address their orders against content considered illegal, according to national and/ or EU law, ii) taking timely, diligent, non-arbitrary and objective action upon receipt of notices by users considering certain content illegal, iii) informing users concerning the measures taken upon receipt of the relevant notice, and iv) publicly reporting about content moderation measures.

In this respect, I note that the DSA obligations apply without exceptions or discrimination to the moderation of the whole user community and content of X (including yourself as a user with over 190 million followers) which is accessible to EU users and should be fulfilled in line with the risk-based approach of the DSA, which requires greater due diligence in case of a foreseeable increase of the risk profile.

As you know, formal proceedings are already ongoing against X under the DSA, notably in areas linked to the dissemination of illegal content and the effectiveness of the measures taken to combat disinformation.

As the relevant content is accessible to EU users and being amplified also in our jurisdiction, we cannot exclude potential spillovers in the EU. Therefore, we are monitoring the potential risks in the EU associated with the dissemination of content that may incite violence, hate and racism in conjunction with major political – or societal – events around the world, including debates and interviews in the context of elections.

Let me clarify that any negative effect of illegal content on X in the EU, which could be attributed to the ineffectiveness of the way in which X applies the relevant provisions of the DSA, may be relevant in the context of the ongoing proceedings and of the overall assessment of X's compliance with EU law. This is in line with what has already been done in the recent past, for example in relation to the repercussions and amplification of terrorist content or content that incites violence, hate and racism in the EU, such as in the context of the recent riots in the United Kingdom.

I therefore urge you to promptly ensure the effectiveness of your systems and to report measures taken to my team.

My services and I will be extremely vigilant to any evidence that points to breaches of the DSA and will not hesitate to make full use of our toolbox, including by adopting interim measures, should it be warranted to protect EU citizens from serious harm.

Yours sincerely,

Thierry Breton

Cc: Linda Yaccarino, CEO of X

Exhibit 17

Letter from Rep. Jim Jordan, Chairman, H.
Comm. on the Judiciary, to Mr. Thierry Breton,
Comm'r for Internal Market, European
Comm'n (Aug. 15, 2024).

ONE HUNDRED EIGHTEENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6216

(202) 225-6906
judiciary.house.gov

August 15, 2024

Mr. Thierry Breton
Commissioner for Internal Markets
European Commission
Rue de la Loi / Wetstraat 200
1049 Brussels, Belgium

Dear Mr. Breton:

The Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government of the U.S. House of Representatives are conducting oversight of how and to what extent the executive branch of the U.S. government has coerced or colluded with companies and other intermediaries to censor lawful speech.¹ As a part of our oversight, the Select Subcommittee has received testimony about how officials from other governments, including you and other officials in the European Union (EU), have sought to censor speech—including political speech—online.² In light of your recent threats of reprisal toward X Corp., an American company, for facilitating political discourse in the United States, we write to demand that you stop any attempt to intimidate individuals or entities engaged in political speech in the United States and that you take no action to otherwise interfere in the American democratic process.

¹ See Ryan Tracy, *Facebook Bowed to White House Pressure, Removed Covid Posts*, WALL ST. J. (July 28, 2023).

² See, e.g., *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Fed. Gov't of the H. Comm. on the Judiciary*, 118th Cong. (Nov. 30, 2023) (submitted written statement of Rupa Subramanya) (“Across the world right now, governments, in the name of the good, are considering or adopting measures like we have in Canada. In Dublin, they’re about to enact a draconian hate-crime bill that poses a dire threat to free speech. In Paris, President Emanuel Macron has called for censoring online speech. **In Brussels, the EU’s Internal Market Commissioner [Thierry Breton] is calling for a crackdown on ‘illegal content.’** In Brasilia, they’re fighting ‘fake news’ and ‘disinformation’ by clamping down on legitimate online speech. To say nothing of Russia and China and Iran. America is so exceptional—indispensable really. Please do not succumb to the same illiberal, the same authoritarianism. Please keep fighting for what you know is right. Canada is watching. *The whole world is watching.*”) (bolded emphasis added; italicized emphasis in original); see also STAFF OF THE H. COMM. ON THE JUDICIARY AND THE SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., *THE ATTACK ON FREE SPEECH ABROAD AND THE BIDEN ADMINISTRATION’S SILENCE: THE CASE OF BRAZIL* (Comm. Print Apr. 17, 2024); STAFF OF THE H. COMM. ON THE JUDICIARY AND THE SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., *THE ATTACK ON FREE SPEECH ABROAD AND THE BIDEN ADMINISTRATION’S SILENCE: THE CASE OF BRAZIL, PART II* (Comm. Print May 7, 2024).

In the United States, government censorship of speech is unacceptable and political speech, in particular, sits at the very core of the First Amendment to the U.S. Constitution.³ Here, political candidates have a right to broadcast their message to voters, and voters have a right to hear from the people running to represent them. Here, government bureaucrats may not intimidate, coerce, or threaten individuals engaged in free speech. Free expression in the marketplace of ideas is a cherished and fundamental American value that sets the United States apart as the world's foremost democracy.

Regrettably, the EU does not share the United States's commitment to free expression in the digital age. The EU's Digital Services Act (DSA), passed in 2022, is Europe's comprehensive internet regulation regime.⁴ It requires so-called "Very Large Online Platforms" operating in the EU, such as X, Facebook, and YouTube, to censor broad and vague categories of online speech, including alleged "misinformation," no matter where the speech originated.⁵ These provisions, if adopted in America, would clearly violate the First Amendment by prohibiting individuals' right to free expression.⁶ The EU law is also bad policy—by manipulating the marketplace of ideas, government coercion, not merit, shapes public debate and the discourse of ideas.⁷ In recent days, you have used these provisions to threaten X with adverse action if the company does not censor constitutionally protected speech originating in the United States.⁸

On August 12, X broadcasted a highly publicized conversation between its owner, Elon Musk, and President Donald Trump, the current Republican nominee in the upcoming election.⁹ Ahead of this interview, you made veiled threats towards Mr. Musk, warning that you "[would] not hesitate" to weaponize your DSA enforcement "toolbox" if you deemed the content of the interview to be "harmful."¹⁰ You wrote to Mr. Musk that even though the interview would take place in United States, you would be "highly vigilant" for "potential spillovers in the EU."¹¹ You

³ See U.S. CONST., amend. I; *Mills v. State of Ala.*, 384 U.S. 214, 218-219 (1966). ("There is practically universal agreement that a major purpose of [the First] Amendment was to protect the free discussion of governmental affairs. This of course includes discussions of candidates . . . and all such matters relating to political processes.").

⁴ Ioanna Tourkochoriti, *The Digital Services Act and the EU as the Global Regulator of the Internet*, 24 CHI. J. INT'L L. 129 (2023).

⁵ *Id.*; see also Jacob Mchangama, *Don't be too tempted by Europe's plan to fix social media*, L.A. TIMES (Dec. 23, 2022) ("The Digital Services Act will essentially oblige Big Tech to act as a privatized censor on behalf of governments – censors who will enjoy wide discretion under vague and subjective standards.").

⁶ J.D. Tuccille, *E.U.'s Digital Services Act Threatens Americans' Free Speech*, REASON (June 5, 2023) (describing how legislative changes in the United States similar to the DSA "would run afoul of the First Amendment").

⁷ See STAFF OF THE H. COMM. ON THE JUDICIARY AND THE SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE CENSORSHIP INDUSTRIAL COMPLEX: HOW TOP BIDEN WHITE HOUSE OFFICIALS COERCED BIG TECH TO CENSOR AMERICANS, TRUE INFORMATION, AND CRITICS OF THE BIDEN ADMINISTRATION (Comm. Print May 1, 2024).

⁸ Thierry Breton (@ThierryBreton), X (Aug. 12, 2024, 12:25 PM), <https://x.com/ThierryBreton/status/1823033048109367549>.

⁹ Donald J. Trump (@realDonaldTrump), X (Aug. 12, 2024, 7:47 PM), <https://x.com/realdonaldtrump/status/1823144316014911820>.

¹⁰ Thierry Breton (@ThierryBreton), X (Aug. 12, 2024, 12:25 PM), <https://x.com/ThierryBreton/status/1823033048109367549>.

¹¹ *Id.*

also approvingly referenced the United Kingdom's recent efforts to arrest citizens for online speech disfavored by government authorities.¹²

As the U.S. election approaches, American voters have the constitutional right to hear from nominees for public office—including President Trump. In the United States, political candidates have the right to express their views and journalists have the right to report and question candidates for public office.¹³ Your recent threats to Mr. Musk and X Corp. for facilitating political discourse in the United States are antithetical to fundamental American values and an inappropriate intrusion in the American democratic process. These actions must stop immediately.

To ensure that the American democratic process is not corrupted by your unilateral regulatory conduct, we request a briefing about (1) the European Commission's efforts to intimidate, threaten, or coerce Elon Musk or X Corp. in connection with Mr. Musk's interview of President Donald Trump; (2) efforts by the European Commission to use EU law to force companies to censor American speech; and (3) any communications the European Commission has had with the Biden-Harris Administration to use EU law as a way to bypass the First Amendment.

We respectfully ask that your staff arrange the briefing as soon as possible but no later than 5:00 p.m. on August 29, 2024. Pursuant to the Rules of the House of Representatives, the Committee on the Judiciary has jurisdiction to conduct oversight of matters concerning "civil liberties" to inform potential legislative reforms.¹⁴ In addition, House Resolution 12 authorized the Committee's Select Subcommittee on the Weaponization of the Federal Government to investigate "issues related to the violation of the civil liberties of citizens of the United States."¹⁵ If you have any questions about this matter, please contact Committee staff at (202) 225-6906.

Sincerely,



Jim Jordan
Chairman

cc: The Honorable Jerrold L. Nadler, Ranking Member

¹² *Id.*

¹³ See *Fighting for a Free Press: Protecting Journalists and their Sources, Hearing of the Subcomm. on the Const. and Limited Gov't. of the H. Comm. on the Judiciary*, 118th Cong. (Apr. 11, 2024).

¹⁴ Rules of the House of Representatives R. X (2023).

¹⁵ H. Res. 12 § 1(b)(1).

Exhibit 18

Letter from Thierry Breton, Comm'r for Internal Market, European Comm'n, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 21, 2024).



EUROPEAN COMMISSION

Thierry Breton
Member of the Commission

Brussels, 21 August 2024

The Honorable Jim Jordan
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515
United States

Dear Chairman Jordan,

I would like to thank the Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government of the U.S. House of Representatives for giving the European Commission the opportunity to dispel some misinterpretations regarding our letter to X on 12 August 2024.

Free speech is a pillar of our European democracy, just as in the United States. The essence of your First Amendment is at the core of the EU Charter of Fundamental Rights and the European Convention on Human Rights, which are legally binding on all EU institutions and 27 Member States, under the judicial control of the European courts. Thus, let me state upfront: contrarily to what has been claimed, nowhere in the letter did we call into question the broadcasting of an interview with a presidential candidate or any similar event. The European Commission would never interfere in the American democratic process or aim to censor freedom of expression, within or beyond its borders. It is ill-founded and simply incorrect to suggest otherwise.

The United States and the EU share many of the same concerns in relation to the societal risks and harms caused by online platforms. In the EU, transparency, accountability, trust, and empowerment of users online are well-established principles, and now enshrined in the Digital Services Act (DSA)¹, a law passed in 2022 by the EU legislature that became applicable in 2023.

The objective of the DSA is to ensure that everyone in the EU can enjoy online platform services safely and in full respect of the fundamental rights which we share, including privacy, dignity, the protection of minors, security, democracy and of course freedom of speech and of information.

¹ Regulation (EU) 2022/2065, OJ L 277, 27.10.2022, p. 1–102.

The DSA does not regulate content. It does not dictate what can or cannot be said online. As in the offline world, that is a matter for specific laws and the courts to determine. What the DSA does is to require online platforms to act responsibly and respect the law, regardless of where they are headquartered, to the extent content on their services is accessible to users in the EU.

Under the DSA, the responsibilities of online platforms increase along with the platform's reach and societal impact, with so-called "Very Large Online Platforms" (i.e. those reaching more than 45 million users in the EU or 10% of the EU population) being subject to the most stringent legal obligations and direct supervision by the European Commission.

The DSA requires online platforms to diligently and objectively enforce their own terms of service, and protects EU users against over-removal of lawful content. Content moderation must be transparent, non-arbitrary, and take due account of freedom of expression. Online platforms must justify the reasons of their content moderation decisions and users are given means to challenge those decisions and ask for redress should their rights have been unduly affected.

Moreover, the DSA requires online platforms to make sure that their algorithmic systems do not amplify illegal content, such as incitation to commit acts of violence, to take effective risk mitigation measures to address the dissemination of such content, to process users' notices on potentially illegal content in a timely, diligent, non-arbitrary and objective manner, and to cooperate with national authorities issuing orders to take down illegal content.

Very Large Online Platforms must also perform annual assessments of the societal risks stemming from the design and use of their service, including addictive design, disinformation and foreign interference, and they must deploy reasonable, proportionate and effective mitigation measures tailored to those risks. Such measures must be carefully balanced against restrictions to the freedom of speech. Public accountability is ensured by the requirement to provide independent researchers and journalists access to data held by such Very Large Online Platforms.

These, in a nutshell, are the obligations that the DSA has introduced to protect the European online world, our citizens, and our democracy.

Even before the entry into force of these new rules, we have been available to help all regulated entities under our supervision – the Very Large Online Platforms – adapt their systems in line with these rules, including through stress tests such as the one mutually agreed with X, which self-reported over 105 million users in the EU, i.e. one third of its user base². In the application of the DSA, the European Commission has maintained a constructive engagement and continues to be open to dialogue with all regulated entities. At the same time, in my role as the Member of the European Commission entrusted with the enforcement of the DSA, I have the duty to ensure strict compliance.

This work has already resulted in several investigations including one into X related, among other things, to the dissemination of illegal content in the EU, and the effectiveness of the measures taken by X to combat information manipulation³.

² The Commission's designation decision can be consulted [here](#).

³ The opening decision can be consulted [here](#). Beyond the investigation against X, six investigations are currently ongoing against TikTok, Meta and AliExpress. Further information on the Commission's supervisory activities is available [here](#).

In this context, we noted that, on 11 August 2024, Mr. Musk announced a likely scale-up of X's user base due to a planned live-streamed event. Any such major scale-up requires not just technical testing, but also diligent analysis of how to ensure that the platform copes with the increased compliance risks entailed by a larger user base.

Major events are indeed likely to generate a spike of a very high intensity of posts, messages, and reactions by users. That is why the DSA requires platforms to have adequate means to deal with massive traffic increase avoiding risks of amplification of any posts by its millions of users potentially containing illegal content, disinformation or which are contrary to the terms and conditions of the platform. In this respect, I note that X's terms of service ban hateful content⁴; they also set rules on the moderation of violent content and to ensure civic integrity⁵.

Unfortunately, these are not theoretical risks. I decided to write to Mr. Musk, recalling the DSA obligations, to ensure that X's trust and safety systems function properly to cope with a likely spike of online activity which could amplify dissemination in the EU of posts by users potentially containing illegal content, disinformation, or posts which run counter to the terms and conditions of the platform.

The letter to X did not raise any issues with the live broadcasting of the interview itself. We take no view on the context of the interview and the political views of the protagonists of that interview are of no relevance in our decision to send that letter. We would send a similar reminder to any of the DSA regulated entities under the Commission's supervision under similar circumstances involving a major scale-up.

We also recall that acts and decisions adopted by the Commission on the basis of the DSA Regulation are taken in full independence and are subject to judicial review.

Finally, as per your question, we can assure you that no communication was exchanged by the European Commission with EU Member States, the U.S., or any other administration in advance of our letter to Mr. Musk.

I trust that these explanations will help address your concerns. The Commission staff is available to brief your staff further if needed.

Yours sincerely,



Thierry Breton

Annex: Letter to X of 12 August 2024

⁴ “[Direct] attack other people on the basis of race, ethnicity, national origin, caste, sexual orientation, gender, gender identity, religious affiliation, age, disability, or serious disease”. See <https://help.x.com/en/rules-and-policies/hateful-conduct-policy>

⁵ See <https://help.x.com/en/rules-and-policies#safety-and-cybercrime>

Exhibit 19

Letter from Rep. Jim Jordan, Chairman, H.
Comm. on the Judiciary, to Mr. Thierry Breton,
Comm'r for Internal Market, European
Comm'n (Sept. 10, 2024).

ONE HUNDRED EIGHTEENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6216

(202) 225-6906
judiciary.house.gov

September 10, 2024

Mr. Thierry Breton
Commissioner for Internal Markets
European Commission
Rue de la Loi / Wetstraat 200
1049 Brussels, Belgium

Dear Mr. Breton:

We received your response to our August 15 letter about your threats of reprisal toward Elon Musk, an American citizen, and X Corp., an American company, for facilitating political discourse in the United States.¹ Your response, however, failed to alleviate our concerns that you may attempt to censor or suppress lawful speech in the United States using the European Union's (EU) Digital Services Act (DSA).² We write to reiterate our position that the EU's burdensome regulation of online speech must not infringe on protected American speech, to note the inaccurate statements in your response, and to accept your offer of a European Commission (EC) staff briefing.

First, your claim that "the DSA does not regulate content" is contradicted by the text of the DSA and by your own actions.³ The DSA, as you admit in your letter, requires "Very Large Online Platforms" (VLOPs), such as X, Facebook, and YouTube, to take "mitigation measures" against alleged "disinformation."⁴ The DSA defines "disinformation" as a type of "content,"⁵ and

¹ Letter from Thierry Breton, Comm'r for Internal Markets, European Comm'n, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 21, 2024).

² Your response also appears to follow a familiar pattern in which you downplay threatening statements after the fact. See Sam Schechner, *Twitter to Face Stress Test This Month, Top EU Tech Regulator Says*, WALL ST. J. (June 1, 2023) ("Breton last week, noting Twitter had withdrawn from a voluntary EU code of conduct on disinformation policies, tweeted: 'You can run but you can't hide,' adding that 'fighting disinformation will be legal obligation under #DSA as of August 25.' 'I'm not threatening anyone,' Breton said during the interview Thursday. 'We are here to help companies comply with our new law.'").

³ Letter from Thierry Breton, Comm'r for Internal Markets, European Comm'n, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 21, 2024).

⁴ *Id.*

⁵ See, e.g., Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 9 (hereinafter "Digital Services Act") ("the dissemination of disinformation or other content"); 84 ("Such providers

because the DSA regulates disinformation,⁶ the DSA—contrary to your claims otherwise—regulates content.⁷ In fact, in your threat letter to Elon Musk, you made clear that the DSA obligates X to censor allegedly “harmful content”—i.e., content disfavored by the EU.⁸ In addition, according to reports, you and a team from the EU visited the headquarters of X (then-Twitter) in San Francisco last year to “review how the company responds to what EU regulators view as problematic tweets, both ones they flag from centers in Europe and ones they don’t” and to “look at why *certain content* might slip through the cracks.”⁹

Your threats against free speech do not occur in a vacuum, and the consequences are not limited to Europe. The harms caused by EU-imposed censorship spill across international borders, as many platforms generally maintain one set of content moderation policies that they apply globally.¹⁰ Thus, the EU’s regulatory censorship regime may limit what content Americans can view in the United States.¹¹ American companies also have an enormous incentive to comply with the DSA and public threats from EU commissioners like you. If these companies fail to censor content deemed by a European official to be “harmful” or “disinformation,” the DSA authorizes the EC to impose a punitive fine of up to six percent of the company’s global revenue—which, for many American companies, would amount to billions of dollars.¹²

should therefore pay particular attention on how their services are used to disseminate or amplify misleading or deceptive content, including disinformation.”). The full text of the DSA specifically refers to “content” in over 100 places.

⁶ Letter from Thierry Breton, Comm’r for Internal Markets, European Comm’n, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 21, 2024) (noting that the DSA requires VLOPs to “perform annual assessments of the societal risks stemming from the design and use of their service, including . . . disinformation,” and to take “mitigation measures” in response.).

⁷ Cf. *id.*; *Questions and answers on the Digital Services Act**, EUROPEAN COMM’N, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348 (last accessed Aug. 30, 2024) ; *see also* Digital Services Act, at ¶¶ 9, 84; Sam Schechner, *Twitter to Face Stress Test This Month, Top EU Tech Regulator Says*, WALL ST. J. (June 1, 2023).

⁸ Thierry Breton (@ThierryBreton), X (Aug. 12, 2024, 12:25 PM), <https://x.com/ThierryBreton/status/1823033048109367549> (emphasis added).

⁹ Sam Schechner, *Twitter to Face Stress Test This Month, Top EU Tech Regulator Says*, WALL ST. J. (June 1, 2023) (emphasis added); *see also id.* (“A team of roughly five to 10 digital specialists from the EU plan to put Twitter, and possibly other companies, through their *content-policing paces* during a visit to San Francisco in late June, Thierry Breton, the bloc’s commissioner for the internal market, said in an interview.”) (emphasis added).

¹⁰ *See, e.g., Facebook Community Standards*, META, <https://transparency.meta.com/policies/community-standards/> (last accessed Aug. 28, 2024) (“Our Community Standards apply to everyone, all around the world, and to all types of content, including AI-generated content.”); *Community Guidelines*, YOUTUBE, <https://www.youtube.com/howyoutubeworks/policies/community-guidelines/#developing-community-guidelines> (last accessed Aug. 28, 2024) (“Each of our policies is carefully thought through so they are consistent, well-informed, and can be applied to content from around the world.”).

¹¹ *See, e.g., Dawn Carla Nunziato, The Digital Services Act and the Brussels Effect on Platform Content Moderation*, 24 CHIC. J. INT. LAW 115 (2023) (“In short, the DSA’s substantive content moderation and notice and take down provisions will likely incentivize the platforms to remove large swaths of content And the platforms will likely alter their globally applicable terms of service and content moderation guidelines in response to the DSA’s mandates in ways that will be speech-restrictive worldwide.”); Jonathan Turley, *Europe’s plot to regulate political speech in America*, THE HILL (Aug. 17, 2024).

¹² Digital Services Act, *supra* note 5, Art. 52 §3; *see also* The Editorial Board, *European Censorship, Elon Musk and the Telegram Arrest*, WALL ST. J. (Aug. 27, 2024).

Second, your assertion that you would “never interfere in the American democratic process” is contradicted by your actions.¹³ You claim that you “decided to write to Mr. Musk [] to ensure that X’s trust and safety systems function properly to cope with a likely spike of online activity which could amplify dissemination in the EU of posts by users potentially containing illegal content, disinformation, or posts which run counter to the terms and conditions of the platform.”¹⁴ However, to the best of our knowledge, you have not sent a similar unsolicited letter concerning “a likely spike in online activity” for any other American political discourse that has been broadcast live on X and that could be alleged to include purported “disinformation” or “harmful content.”¹⁵ If you have sent such an unsolicited letter, you certainly did not do so in such a public manner as you did with your letter to Musk. The only logical inference from your actions is that your letter was intended as a threat to Musk that the EU would, as you warned, “make full use of [its] toolbox” if he facilitated political speech with which you disagreed.¹⁶

Your letter, and for that matter the EC and the DSA, seems to miss a fundamental point about free speech—to oppose censorship of so-called “disinformation” is not to defend or to endorse the content. It is to respect the right and the ability of citizens to consume content and to make decisions about what speech is persuasive, what is truthful, and what is accurate. To oppose censorship is to acknowledge that a government with the authority to define disinformation will inevitably do so in a way that benefits those in power at the expense of the truth.¹⁷ As demonstrated by your letter, EU officials are not above factual mistakes and

¹³ See The Editorial Board, *European Censorship, Elon Musk and the Telegram Arrest*, WALL ST. J. (Aug. 27, 2024) (“Thierry Breton, the European Commissioner for Internal Market and a former French telecom executive, is wielding the law as a cudgel to censor speech worldwide. Consider his threat against Mr. Musk mere hours before Mr. Musk’s recent live interview on X.com with Donald Trump. [] This is thuggish stuff. European regulators are trying to meddle in the U.S. presidential election.”).

¹⁴ Letter from Thierry Breton, Comm’r for Internal Markets, European Comm’n, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 21, 2024).

¹⁵ See, e.g., Noah Rothman, *Kamala Harris’s Tough-on-Crime Story Is Nothing Like Her Actual Record*, NAT. REV. (Aug. 30, 2024); Tyler O’Neil, *5 Massive Lies at the Democratic National Convention*, THE DAILY SIGNAL (Aug. 22, 2024); Paul du Quenoy, *Biden Took to the Stage, and Lied, and Lied, and Lied | Opinion*, NEWSWEEK (Aug. 20, 2024).

¹⁶ Letter from Thierry Breton, Comm’r for Internal Markets, European Comm’n, to Elon Musk, Owner, X Corp. (Aug. 12, 2024).

¹⁷ See also *Hearing on the Weaponization of the Federal Government Before the Select Subcomm. of the Weaponization of the Fed. Gov’t of the H. Comm on the Judiciary*, 118th Cong. (Mar. 9, 2023) (testimony of Matt Taibbi) (“One of my heroes growing up was the Ukraine-born author Isaac Babel. He gave a speech at the first Soviet Writers Congress, and he was asked if any important rights had been taken away. He sarcastically answered, ‘No. The only rights that have been taken away are the right to be wrong.’ The crowd laughed, but he was making an important point, which is that in a free country you can’t have freedom without the freedom to be wrong.”).

misunderstandings.¹⁸ Dissenting voices matter because the “expert consensus” is often wrong, as shown most recently by the devastating consequences of the government-imposed lockdowns.¹⁹

Accordingly, the Committee and Select Subcommittee accept your offer for EC staff to provide a briefing. As noted in our first letter, please have your staff prepared to provide additional information on (1) the European Commission’s efforts to intimidate, threaten, or coerce Elon Musk or X Corp. in connection with Mr. Musk’s interview of President Donald Trump; (2) efforts by the European Commission to use EU law to force American companies to censor American speech; and (3) any communications the European Commission has had with the Biden-Harris Administration to use EU law as a way to bypass the First Amendment. Please have your staff arrange the briefing as soon as possible but no later than 10:00 a.m. ET on September 24, 2024. If you have any questions about this matter, please contact Committee staff at (202) 225-6906.

Sincerely,



Jim Jordan
Chairman

cc: The Honorable Jerrold L. Nadler
Ranking Member

¹⁸ Compare Letter from Thierry Breton, Comm’r for Internal Markets, European Comm’n, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 21, 2024) (“The DSA does not regulate content” and “The European Commission would never interfere in the American democratic process or aim to censor freedom of expression, within or beyond its borders.”), with *supra*, note 5 (“The full text of the DSA specifically refers to ‘content’ in over 100 places.”), and Letter from Thierry Breton, Comm’r for Internal Markets, European Comm’n, to Elon Musk (Aug. 12, 2024) (“DSA obligations apply without exceptions or discrimination to the moderation of the whole user community and content of X (including yourself as a user with over 190 million followers) which is accessible to EU users”), and Letter from Thierry Breton, Comm’r for Internal Markets, European Comm’n, to Elon Musk (Aug. 12, 2024) (threatening to “make full use of our toolbox” if Elon Musk facilitated political speech with which you disagreed).

¹⁹ See, e.g., Great Barrington Declaration (Oct. 4, 2020) (explaining how COVID-19 lockdown policies were producing devastating effects on short and long-term public health); The Editorial Board, *The Startling Evidence on Learning Loss Is In*, N.Y. TIMES (Nov. 18, 2023) (“The school closures that took 50 million children out of classrooms at the start of the pandemic may prove to be the most damaging disruption in the history of American education.”); Peter C. Earle et al., *The Devastating Economic Impact of Covid-19 Shutdowns*, AM. INST. FOR ECONOMIC RESEARCH (“Whether policymakers purposely or out of ignorance disregarded them, the tradeoffs of stay-at-home orders were immediate and severe: a massive spike in unemployment, rivaling the Great Depression; similarly historic drops in GDP, and others.”); Nafiso Ahmed et al., Mental health in Europe during the COVID-19 pandemic: a systematic review, 10 LANCET PSYCH. 537 (2023) (“Potential consequences of the pandemic and associated social restrictions included increase in psychological distress, increase in new onsets of mental health conditions, and worsening of difficulties already experienced by people living with mental health conditions.”); Sylke V. Schnepf et al., *COVID-19 and the European Education Performance Decline: A Focus on Primary School Children’s Reading Achievement between 2016 and 2021*, IZA DP No. 16531 (2023) (“It is widely acknowledged that COVID-induced physical school closure lead to considerable learning loss.”).

Exhibit 20

Letter from Rep. Jim Jordan, Chairman, H.
Comm. on the Judiciary, to Ms. Henna
Virkkunen, Exec. Vice-President for Tech
Sovereignty, Security, and Democracy,
European Comm'n (Jan. 31, 2025).

ONE HUNDRED NINETEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6216

(202) 225-6906
judiciary.house.gov

January 31, 2025

Ms. Henna Virkkunen
Executive Vice-President for Tech Sovereignty, Security, and Democracy
European Commission
Rue de la Loi / Wetstraat 200
1049 Brussels, Belgium

Dear Ms. Virkkunen:

The Committee on the Judiciary of the U.S. House of Representatives is conducting oversight of how and to what extent foreign laws, regulations, and judicial orders compel or coerce companies to censor speech in the United States.¹ As part of this oversight, the Committee has examined how officials from other governments, such as the European Union (EU), have sought to censor speech online.² We previously wrote to your predecessor, Thierry Breton, following his threats of reprisal toward an American company for facilitating political discourse in the United States.³ In light of your recent confirmation as the European Commission's (EC) Executive Vice-President for Tech Sovereignty, Security, and Democracy, the Commissioner responsible for enforcing the EU's Digital Services Act (DSA), we write to express our serious concerns with how the DSA's censorship provisions affect free speech in the United States.⁴ In addition, consistent with the EC's previous engagement with the Committee,

¹ See, e.g., Peter Caddle, *EU must not to 'interfere in US politics' through tech censorship, justice committee warns*, BRUSSELS SIGNAL (Aug. 19, 2024); Peter Caddle, *US Congressman makes fresh attack on Breton, warns 'digital enforcer' not to censor Americans*, BRUSSELS SIGNAL (Sept. 10, 2024); see also Steven Lee Myers, *E.U. Law Sets the Stage for a Clash Over Disinformation*, N.Y. TIMES (Sept. 27, 2023) ("The law, the Digital Services Act, is intended to force social media giants to adopt new policies and practices If the measure is successful, as officials and experts hope, its effects could extend far beyond Europe, changing company policies in the United States and elsewhere.").

² See, e.g., *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Fed. Gov't of the H. Comm. on the Judiciary*, 118th Cong. (Nov. 30, 2023) (submitted written statement of Rupa Subramanya).

³ See Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Thierry Breton, Comm'r for Internal Mkts., European Comm'n (Aug. 15, 2024); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary to Thierry Breton, Comm'r for Internal Mkts., European Comm'n (Sept. 10, 2024).

⁴ Mission Letter from Ursula von der Leyen, President, European Comm'n, to Henna Virkkunen, Exec. Vice-President for Tech Sovereignty, Security, and Democracy, European Comm'n (Sept. 17, 2024), at 7.

we request a briefing on your approach to DSA enforcement and ongoing investigations of American companies.⁵

The DSA requires that social media platforms have systematic processes to remove “misleading or deceptive content,” including so-called “disinformation,” even when such content “is not illegal.”⁶ Though nominally applicable to only EU speech, the DSA, as written, may limit or restrict Americans’ constitutionally protected speech in the United States.⁷ Companies that censor an insufficient amount of “misleading or deceptive” speech—as defined by EU bureaucrats—face fines up to six percent of global revenue, which would amount to billions of dollars for many American companies.⁸ Furthermore, because many social media platforms generally maintain one set of content moderation policies that they apply globally, restrictive censorship laws like the DSA may set *de facto* global censorship standards.⁹

Indeed, the establishment of a global censorship law appears to be the DSA’s very purpose.¹⁰ Your predecessor, Thierry Breton, demonstrated this when he attempted to weaponize the DSA to pressure American companies to censor American speech in the United States.¹¹ In August 2024, Breton publicly threatened an American social media company with adverse regulatory action if the company did not censor American content to prevent “potential spillovers in the EU.”¹² Likewise, your recent statements raise serious concerns that you are following Mr. Breton’s footsteps. In your confirmation hearing, you promised vigorous enforcement of the

⁵ Staff of European Comm’n, Briefing to Staff of H. Comm. on the Judiciary (Oct. 2, 2024).

⁶ See, e.g., Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 9, 84, Art. 35.

⁷ See, e.g., STAFF OF THE SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF THE FEDERAL GOVERNMENT (Comm. Print Dec. 20, 2024), at 1988-2618; see also Steven Lee Myers, *E.U. Law Sets the Stage for a Clash Over Disinformation*, N.Y. TIMES (Sept. 27, 2023).

⁸ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277), Art. 52 §3; see also The Editorial Board, *European Censorship, Elon Musk and the Telegram Arrest*, WALL ST. J. (Aug. 27, 2024).

⁹ See, e.g., Dawn Carla Nunziato, *The Digital Services Act and the Brussels Effect on Platform Content Moderation*, 24 CHIC. J. INT. LAW 115 (2023). (“In short, the DSA’s substantive content moderation and notice and take down provisions will likely incentivize the platforms to remove large swaths of content . . . And the platforms will likely alter their globally applicable terms of service and content moderation guidelines in response to the DSA’s mandates in ways that will be speech-restrictive worldwide.”).

¹⁰ See, e.g., *id.*; Steven Lee Myers, *E.U. Law Sets the Stage for a Clash Over Disinformation*, N.Y. TIMES (Sept. 27, 2023) (“The law, the Digital Services Act, is intended to force social media giants to adopt new policies and practices . . . If the measure is successful, as officials and experts hope, its effects could extend far beyond Europe, changing company policies in the United States and elsewhere.”).

¹¹ See Thierry Breton (@ThierryBreton), X (Aug. 12, 2024, 12:25 PM), <https://x.com/ThierryBreton/status/1823033048109367549>; see also The Editorial Board, *European Censorship, Elon Musk and the Telegram Arrest*, WALL ST. J. (Aug. 27, 2024) (“Thierry Breton, the European Commissioner for Internal Market and a former French telecom executive, is wielding the law as a cudgel to censor speech worldwide. Consider his threat against Mr. Musk mere hours before Mr. Musk’s recent live interview on X.com with Donald Trump. [] This is thuggish stuff. European regulators are trying to meddle in the U.S. presidential election.”).

¹² Thierry Breton (@ThierryBreton), X (Aug. 12, 2024, 12:25 PM), <https://x.com/ThierryBreton/status/1823033048109367549>.

DSA against American companies.¹³ In a recent opinion approving a new social media Hate Speech Code of Conduct, you endorsed a censorship-by-proxy campaign in which social media companies are required to give priority treatment to censorship requests from government-backed third parties—a scheme similar to one the Committee previously uncovered, and stopped, in the United States.¹⁴ Relatedly, in written answers in your Commissioner-designate questionnaire, you expressed support for EU President Ursula von der Leyen’s Democracy Shield proposal,¹⁵ which involves setting up an EU agency “to detect, track, and delete [allegedly] deceitful online content in coordination with national agencies.”¹⁶

Attempts to censor so-called “disinformation,” as you seem intent to do, miss the fundamental point about free speech. To oppose censorship is to acknowledge that a government with the authority to define disinformation will inevitably do so in a way that benefits those in power at the expense of the truth.¹⁷ No entity has a monopoly on good ideas. Dissenting voices matter because the “expert consensus” can be, and often is, wrong, as shown most recently by the devastating consequences of government-imposed lockdowns.¹⁸ In liberal nations like the

¹³ *Confirmation Hearing of Henna Virkkunen, Commissioner-designate, Tech Sovereignty, Security and Democracy: Hearing Before the Comm. on Industry, Rsch., and Energy & Comm. on Internal Mkt. and Consumer Protection of the European Parliament* (Nov. 12, 2024) at 13-16.

¹⁴ European Comm’n, *Commission Opinion of 20.1.2025 on the assessment of the Code of conduct on countering illegal hate speech online + within the meaning of Article 45 of Regulation 2022/2065*, C(2025) 446 final; see STAFF OF THE H. COMM. ON THE JUDICIARY AND THE SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., *THE WEAPONIZATION OF “DISINFORMATION” PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ POLITICAL SPEECH* (Comm. Print Nov. 6, 2023) (detailing the U.S. government’s work with Stanford University’s Election Integrity Partnership to censor Americans in the lead-up to the 2020 U.S. presidential election).

¹⁵ European Parliament, *Responses to Questionnaire to the Commissioner-Designate, Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security, and Democracy*, at 11.

¹⁶ Irene Sanchez & Giorgos Verdi, *Digital deceptions: How a European Democracy Shield can help tackle Russian disinformation*, EUROPEAN COUNCIL ON FOREIGN RELS. (May 28, 2024); see also Mared Gwyn Jones, *Von der Leyen pitches plan to shield EU from foreign interference if re-elected*, EURO NEWS (May 14, 2024) (“The Shield would be tasked with detecting and removing online disinformation[.]”); Ursula von der Leyen (@vonderleyen_epp), X (May 20, 2024, 10:54 AM), https://x.com/vonderleyen_epp/status/1792569693242352120 (“This new structure will track down information manipulation and coordinate with national agencies. The Shield will detect foreign interference, remove content, with a stronger approach to AI deepfakes, and finally pre-bunk and build resilience.”).

¹⁷ See *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary*, 118th Cong. (July 20, 2023) (testimony of Robert F. Kennedy, Jr.) (“There’s never been a time in history when we look back and the guys who were censoring people were the good guys.”).

¹⁸ See, e.g., Great Barrington Declaration (Oct. 4, 2020) (explaining how COVID-19 lockdown policies were producing devastating effects on short and long-term public health); The Editorial Board, *The Startling Evidence on Learning Loss Is In*, N.Y. TIMES (Nov. 18, 2023) (“The school closures that took 50 million children out of classrooms at the start of the pandemic may prove to be the most damaging disruption in the history of American education.”); Peter C. Earle et al., *The Devastating Economic Impact of Covid-19 Shutdowns*, AM. INST. FOR ECONOMIC RSCH. (2020) (“Whether policymakers purposely or out of ignorance disregarded them, the tradeoffs of stay-at-home orders were immediate and severe: a massive spike in unemployment, rivaling the Great Depression; similarly historic drops in GDP, and others.”); Nafiso Ahmed et al., *Mental health in Europe during the COVID-19 pandemic: a systematic review*, 10 LANCET PSYCH. 537 (2023) (“Potential consequences of the pandemic and associated social restrictions included increase in psychological distress, increase in new onsets of mental health

United States and those in the EU, we must respect the right and the ability of citizens to consume content and to make decisions about what speech is persuasive, what is truthful, and what is accurate.¹⁹ By enshrining and protecting freedom of speech, the U.S. Constitution entrusts Americans with the liberty to make these determinations; the DSA, in contrast, seeks to take this power from ordinary people and put it in the hands of governing authorities.²⁰

Accordingly, the Committee asks for a briefing on your approach to DSA enforcement and ongoing DSA proceedings against American companies. Please have your staff arrange the briefing as soon as possible but no later than 10:00 a.m. ET on February 13, 2025. Pursuant to the Rules of the House of Representatives, the Committee on the Judiciary has jurisdiction to conduct oversight of matters concerning “civil liberties” to inform potential legislative reforms.²¹ If you have any questions about this matter, please contact Committee staff at +1 (202) 225-6906.

Sincerely,



Jim Jordan
Chairman

cc: The Honorable Jamie Raskin, Ranking Member

conditions, and worsening of difficulties already experienced by people living with mental health conditions.”); Sylke V. Schnepf & Silvia Granato, *COVID-19 and the European Education Performance Decline: A Focus on Primary School Children’s Reading Achievement between 2016 and 2021*, IZA DP No. 16531 (2023) (“It is widely acknowledged that COVID-induced physical school closure lead to considerable learning loss.”).

¹⁹ See *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. of the Weaponization of the Fed. Gov’t of the H. Comm on the Judiciary*, 118th Cong. (Mar. 9, 2023) (testimony of Matt Taibbi) (“One of my heroes growing up was the Ukraine-born author Isaac Babel. He gave a speech at the first Soviet Writers Congress, and he was asked if any important rights had been taken away. He sarcastically answered, ‘No. The only rights that have been taken away are the right to be wrong.’ The crowd laughed, but he was making an important point, which is that in a free country you can’t have freedom without the freedom to be wrong.”).

²⁰ See *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. of the Weaponization of the Fed. Gov’t of the H. Comm on the Judiciary*, 118th Cong. (Nov. 30, 2023) (submitted written statement of Matt Taibbi) (“This leads to the one inescapable question about new ‘anti-disinformation’ programs that is never discussed, but must be: who does this work? Stanford’s Election Integrity Project helpfully made a graphic showing the ‘external stakeholders’ in their content review operation. It showed four columns: government, civil society, platforms, media. One group is conspicuously absent from that list: ordinary people. Whether America continues the informal *sub rosa* censorship system seen in the Twitter Files or formally adopts something like Europe’s draconian new Digital Services Act, it’s already clear who *won’t* be involved. There’ll be no dockworkers doing content flagging, no poor people from inner city neighborhoods, no single moms pulling multiple waitressing jobs, no immigrant store owners or Uber drivers, etc. These programs will always feature a tiny, rarefied sliver of affluent professional-class America censoring a huge and ever-expanding pool of everyone else.”).

²¹ Rules of the House of Representatives, R. X (2025).

Exhibit 21

Letter from Ms. Henna Virkkunen, Exec.
Vice-President for Tech Sovereignty,
Security, and Democracy, European
Comm'n, to Rep. Jim Jordan, Chairman,
H. Comm. on the Judiciary (Feb. 18,
2025).



EUROPEAN COMMISSION

Henna Virkkunen
Executive Vice-President

Brussels
CA.3/HV/S.2784603

Subject: The EU's Digital Services Act

Dear Mr Chairman,

Thank you for your letter dated 31 January 2025.

I am convinced that the European Union and the United States have a common interest in advancing democracy, the rule of law and human rights, including freedom of speech. I therefore welcome the opportunity to engage with you, the Committee, the U.S. Congress more broadly and the U.S. Administration.

As the newly appointed Executive Vice-President for Tech Sovereignty, Security and Democracy in the European Commission, my mission is to advance digital and frontier technologies in Europe, while strengthening the EU's ability to protect and promote our fundamental values, addressing the complex security threats the EU is facing, upholding the rule of law and our democracy, and protecting the rights of our citizens. Regarding all these responsibilities I am committed to applying the rules in the EU with impartiality.

In reply to your letter, I would like to clarify at the outset that **the Digital Services Act (DSA) applies exclusively within the European Union**. It has no extraterritorial jurisdiction in the U.S. or any other non-EU country.

1. Freedom of speech

I want to be very clear: **the DSA does not regulate speech**. The DSA is content-agnostic, and so is the European Commission and Member States as regulators, which have no power to moderate content or to impose any specific approach to moderation. The substantive rules on unlawful speech or other content (e.g. on child abuse material, illegal hate speech

The Honourable Jim Jordan
Chairman
Congress of the United States
House of Representatives
Committee on the Judiciary

or incitement to terrorism) are established elsewhere, in other pieces of national or EU legislation.

On the contrary, the DSA **guarantees the fundamental right of free speech** by ensuring that online platforms act with transparency and accountability when dealing with users' content. The DSA safeguards free speech by regulating what due process means in the online world: it clarifies the rights of users and establishes what online platforms are required to do, as online intermediaries, when they take decisions affecting online content. This is a simple but essential process to ensure that content is not arbitrarily removed. When platforms remove or demote content, they must inform the user that posted the content, explain why they took the decision, and offer the user the opportunity to challenge that decision. To empower users in their information environment, and help in the fight against crime, online platforms must also offer users the means to signal illegal content encountered on the platform, for example, child sexual abuse material.

The EU is deeply committed to protecting and promoting free speech online and offline, resonating with the same fundamental values of the First Amendment to the U.S. Constitution. The EU Charter of Fundamental Rights is an expression of the rights and freedoms that the Union and its Member States hold in common and '**freedom of expression and information**' is enshrined therein. That freedom guarantees the 'freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

Our perspective on free speech is shaped by historical experience. Many Europeans have living memories of censorship and persecution during the Cold War under communist regimes and other authoritarian regimes of the past century, where freedom of speech did not exist. The EU was founded to secure and uphold democratic freedoms that have been denied in the past.

Protecting all these freedoms remains at the heart of our legal framework and enforcement actions, and the DSA was designed in that spirit.

2. Aim of the DSA and possible misconceptions

I trust that we converge on many aspects of the regulatory objectives of the DSA. This is why I want to address up-front some points that appear to be misconceptions of what the rules say, and what they do not say.

Some concerns have been raised that the DSA might be used to pressure online platforms into restricting lawful speech in the U.S. or elsewhere. **This is categorically not the case.** The DSA does not require online platforms to remove lawful speech and, as explained above, does not apply in the U.S. or other third countries.

On the contrary, the DSA requires online platforms to disclose their content moderation policies to users up front and to put in place mechanisms to ensure that they do not take arbitrary or discriminatory decisions when they enforce those policies. The DSA provides users with several avenues to appeal content moderation decisions and ensures that users can understand why platforms recommend content to them. Online platforms that reach more than 45 million active users (10% of the EU's population) are subject to additional process protections and a 'duty of care' commensurate with their important role in our societies. They must, in addition, set out how they assess and mitigate a number of risks, such as those related to the dissemination of illegal goods and the protection of children, and they must publish those assessments for public scrutiny.

The DSA's transparency provisions, obliging online platforms *inter alia* to file all content moderation decisions in a public database have brought a true step-change in the ability to independently scrutinise and understand the content moderation policies of online platforms. This represents a strong contribution to the cause of freedom of speech.

In Europe, it is our belief that **it should not be up to politicians, executives or private companies to take decisions on what citizens have the right to see or say online**. I agree that no one has a monopoly on the truth. This is why the EU legislature adopted a content-neutral general legal framework to protect freedom of expression, while at the same time providing specific safeguards, e.g. for the well-being of minors online. The enforcement of that EU legal framework is diligent, objective and non-partisan – and all decisions can be challenged before the courts.

The DSA also values self-regulatory measures that the companies themselves adopt to make their own decision making more transparent. There is, for example, a voluntary Code of Conduct signed by a large number of online platforms on illegal hate speech, also referenced in your letter. We are ready to clarify its scope to prevent any misunderstanding.

I hope that these clarifications make clear that far from restricting freedom of speech, the DSA empowers users to better make their own assessment of the content they receive. It is surely the case that the real threats to free expression lie elsewhere. Countries such as Russia, Iran and China impose heavy restrictions on what people can see and what they can say. They also seek to interfere in our own democratic societies, through manipulation of the information space, often directly targeting elections. We do not believe that democratic societies should be passive in the face of such interference, which is why we are developing the EU Democracy Shield referred to in your letter. I know these threats are equally present in the U.S. debate and have led Congress to take action. We would welcome a constructive discussion with the House of Representatives on these shared concerns.

I trust my letter has provided you with the necessary clarifications. I understand that members of my team have already provided briefings to your committee, both in Washington and Brussels. The EU Delegation in Washington stands ready to arrange a further briefing at your convenience to address any further questions you may have regarding DSA enforcement.

I appreciate your attention to these important matters and look forward to constructive discussions in the spirit of our longstanding transatlantic partnership.

Yours sincerely,



Henna VIRKKUNEN

Exhibit 22

Letter from Rep. Jim Jordan, Chairman,
H. Comm. on the Judiciary, to Ms.
Ursula von der Leyen, President,
European Comm'n (Feb. 27, 2025).

ONE HUNDRED NINETEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6216

(202) 225-6906
judiciary.house.gov

February 27, 2025

Ms. Ursula von der Leyen
President
European Commission
Rue de la Loi / Wetstraat 200
1049 Brussels, Belgium

Dear President von der Leyen:

The Committee on the Judiciary of the U.S. House of Representatives is conducting oversight of how and to what extent foreign laws, regulations, and judicial orders compel or coerce companies to censor speech in the United States.¹ As part of this oversight, on February 26, 2025, the Committee issued subpoenas to eight technology companies operating in the United States, requiring them to produce communications with the European Commission (EC) and other European governance bodies related to content moderation or suppression of speech on social media.² We write today to notify you that we expect to receive communications sent or received by EC officials over the coming weeks and months on an ongoing basis. As we assess this material, we respectfully urge the EC to rededicate itself to the fundamental principle of free expression and the notion that the solution to so-called “bad” speech is not enforced silence but additional speech.³

The Committee is concerned by the proliferation of foreign censorship laws, regulations, and judicial orders that threaten Americans’ constitutionally protected right to speak freely online.⁴ For example, the EU’s Digital Services Act (DSA) requires social media and other

¹ See Pieter Haeck, *US presses Brussels for answers over EU social media law*, POLITICO (Jan. 31, 2025); Peter Caddle, *US Congressman makes fresh attack on Breton, warns ‘digital enforcer’ not to censor Americans*, BRUSSELS SIGNAL (Sept. 10, 2024); Peter Caddle, *EU must not to ‘interfere in US politics’ through tech censorship, justice committee warns*, BRUSSELS SIGNAL (Aug. 19, 2024).

² See, e.g., Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Sundar Pichai, CEO, Alphabet (Feb. 26, 2025) (attaching subpoena). The eight companies are Alphabet, Amazon, Apple, Meta, Microsoft, Rumble, TikTok, and X.

³ See, e.g., *Whitney v. California*, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring) (“If there be time to expose through discussion, the falsehood and fallacies, to avert the evil by the processes of education, the remedy to be applied is more speech, not enforced silence.”).

⁴ See Steven Lee Myers, *E.U. Law Sets the Stage for a Clash Over Disinformation*, N.Y. TIMES (Sept. 27, 2023) (“The law, the Digital Services Act, is intended to force social media giants to adopt new policies and practices If the measure is successful, as officials and experts hope, its effects could extend far beyond Europe, changing company policies in the United States and elsewhere.”).

online platforms to have systematic processes to remove “misleading or deceptive content,” including so-called “disinformation,” even when such content “is not illegal,” or else face fines amounting to billions of dollars.⁵ Europe’s censorship efforts may harm Americans’ ability to speak freely online: because many social media platforms generally maintain one set of content moderation policies that they apply globally, the most restrictive censorship laws may set *de facto* global censorship standards.⁶ Indeed, global censorship appears to be the purpose of the DSA.⁷ In August 2024, then-European Commissioner for Internal Market and Services Thierry Breton publicly threatened regulatory retaliation against X Corp. if it permitted American political speech to “spillover[]” into the EU.⁸

For these reasons, the Committee issued subpoenas to technology companies operating in the U.S. for all communications with European government officials regarding content moderation or suppression of speech on social media.⁹ These subpoenas are “continuing in nature,” meaning that they apply to past and future communications.¹⁰ These companies will begin producing documents to the Committee shortly. We write as a courtesy to notify you that the Committee will begin to receive communications with EC officials and to invite you to supplement our record with additional information you believe is relevant to our understanding of the EC’s censorship regime.

The Committee will do everything in its power to protect Americans’ free speech rights, including developing legislative solutions to counter foreign attempts to interfere in America’s marketplace of ideas.¹¹ Pursuant to the Rules of the House of Representatives, the Committee on the Judiciary has jurisdiction to conduct oversight of matters concerning “civil liberties” to inform potential legislative reforms.¹² If you have any questions about this matter, please contact Committee staff at +1 (202) 225-6906.

⁵ See Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 9, 84, Art. 35, Art. 52.

⁶ See, e.g., Dawn Carla Nunziato, *The Digital Services Act and the Brussels Effect on Platform Content Moderation*, 24 CHIC. J. INT. LAW 115 (2023). (“In short, the DSA’s substantive content moderation and notice and take down provisions will likely incentivize the platforms to remove large swaths of content . . . And the platforms will likely alter their globally applicable terms of service and content moderation guidelines in response to the DSA’s mandates in ways that will be speech-restrictive worldwide.”).

⁷ See, e.g., Steven Lee Myers, *E.U. Law Sets the Stage for a Clash Over Disinformation*, N.Y. TIMES (Sept. 27, 2023) (“The law, the Digital Services Act, is intended to force social media giants to adopt new policies and practices If the measure is successful, as officials and experts hope, its effects could extend far beyond Europe, changing company policies in the United States and elsewhere.”).

⁸ Letter from Thierry Breton, Comm’r for Internal Mkts., European Comm’n, to Elon Musk, Owner, X Corp. (Aug. 12, 2024).

⁹ See, e.g., Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Sundar Pichai, CEO, Alphabet (Feb. 26, 2025) (attaching subpoena).

¹⁰ *Id.*

¹¹ See, e.g., No Censors on our Shores Act, H.R. 1071, 119th Cong. (2025).

¹² Rules of the House of Representatives, R. X (2025).

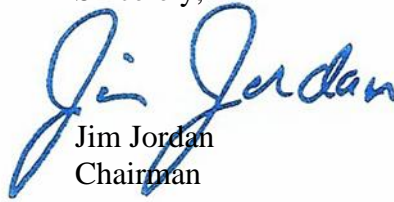
President Ursula von der Leyen

February 27, 2025

Page 3

Thank you for your attention to this matter.

Sincerely,



Jim Jordan
Chairman

cc: Ms. Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security, and
Democracy, European Commission

The Honorable Jamie Raskin, Ranking Member