

RESPONSIBILITY OF ONLINE PLATFORMS FOR THIRD-PARTY CONTENT: A COMPARATIVE ANALYSIS OF THE EU DIGITAL SERVICES ACT AND THE US SECTION 230

Igor Britchenko

University of the National Education Commission

Krakow, Poland

<https://orcid.org/0000-0002-9196-8740>

igor_britchenko@pltech-sci.com

ABSTRACT. This article provides a comprehensive comparative analysis of the two dominant Western regulatory models governing the liability of online platforms for third-party content: the European Union’s Digital Services Act (DSA) and Section 230 of the United States Communications Decency Act (CDA). The analysis employs a comparative legal methodology to dissect the legal architecture, enforcement mechanisms, and underlying jurisprudential philosophies of each regime. It finds that the DSA represents a proactive, systems-based model of co-regulation rooted in a philosophy of ‘digital constitutionalism’, which imposes tiered, affirmative due diligence obligations on platforms to mitigate systemic risks and protect users’ fundamental rights. In contrast, Section 230 embodies a reactive, immunity-based model grounded in the ‘marketplace of ideas’ tradition, providing a broad liability shield to foster innovation and protect free expression, with minimal affirmative duties. The article examines seminal case law, including *Zeran v. America Online, Inc.* and the Supreme Court’s inconclusive ruling in *Gonzalez v. Google, LLC*, alongside the DSA’s early enforcement actions against platforms such as X and Meta. It concludes that the two frameworks are predicated on fundamentally incompatible theories of harm—systemic risk versus individual tort—making direct convergence unlikely. The DSA’s most significant long-term impact may be the establishment of a permanent institutional capacity for regulatory oversight in the EU, a development with no parallel in the US, suggesting a widening transatlantic divergence in platform governance. Future challenges, particularly the rise of generative AI and decentralised platforms, will further test the resilience and adaptability of both models.

Keywords: Digital Services Act (DSA), Section 230, Intermediary Liability, Content Moderation, Platform Governance, Comparative Law, Digital Constitutionalism

1. INTRODUCTION

The digital transformation of the past two decades has been defined by the ascendancy of online platforms. Initially conceived as mere conduits for information, intermediary services have evolved into indispensable components of the global economy and the daily lives of citizens worldwide (European Commission, n.d.-b). Platforms such as social networks, online marketplaces, and content-sharing services have become the new quasi-public squares, shaping public discourse, facilitating commerce, and mediating social interaction on an unprecedented scale (European Commission, 2020; European Commission, n.d.-d).

This exponential growth, however, has precipitated a profound crisis of content governance. The very architectures that enable seamless communication and connection have also become vectors for the proliferation of illegal and harmful content, including disinformation, hate speech, terrorist propaganda, cyberbullying, and the sale of counterfeit or dangerous goods (European Commission, 2020; European Commission, n.d.-d; European Commission, n.d.-e). The societal risks emanating from these platforms are significant, posing tangible threats to the integrity of democratic processes, the protection of fundamental rights, and public safety and health (European Commission, n.d.-b; European Commission, n.d.-d). This context has created an urgent and globally acknowledged need for a coherent legal framework to govern platform responsibility. The central challenge is not merely a technical problem of moderating content at scale, but a fundamental crisis of legitimacy for both state and corporate actors. States are grappling with the limits of their sovereignty in a borderless digital domain, while platforms, which have emerged as powerful private rule-makers, lack the democratic legitimacy to unilaterally govern vast swathes of public life (European Commission, n.d.-d). The regulatory frameworks examined in this article represent two distinct attempts to resolve this legitimacy crisis.

At the heart of the platform governance debate lies a persistent legal and philosophical tension: the need to balance the protection of free expression and the fostering of innovation against the imperative to ensure user safety and hold powerful corporate actors accountable for the harms facilitated by their services (epicenter.works, 2019; Olakoyenikan, 2024; Zelman, 2023). Different legal traditions have struck this balance in markedly different ways, giving rise to two principal legislative models in the Western world. The first is the proactive, risk-based regulatory framework of the European Union, epitomised by the Digital Services Act (DSA), which came into full force in February 2024 (Liberties, 2025). The second is the reactive, immunity-based doctrine of the United States, established by Section 230 of the Communications Decency Act of 1996 (CDA) (47 U.S.C. § 230, 2024; Dickinson, 2024). These two statutes embody divergent approaches to assigning responsibility for third-party content, reflecting a deep-seated transatlantic divide on the role of the state, the market, and the individual in the digital age.

A comparative legal analysis of the DSA and Section 230 is not merely an academic exercise in juxtaposing statutory provisions; it is essential for understanding the future trajectory of global internet governance (Dothan, 2014; Eberle, n.d.). While a substantial body of literature exists on each regime individually, a systematic and in-depth analysis of their divergent philosophical underpinnings and practical consequences remains a critical research gap. Such a comparison reveals how two of the world's most influential legal-economic blocs are constructing conflicting paradigms for the digital economy. This divergence has profound implications for global platforms, which must navigate these competing legal realities, and raises the prospect of the EU's comprehensive regulatory standards becoming a *de facto* global benchmark (Reddit, n.d.). This article seeks to fill this gap by moving beyond a descriptive comparison of rules to a deeper analytical inquiry into how these two frameworks attempt to re-establish legitimate governance in the digital sphere. The EU's approach represents a deliberate effort to impose public-law values onto private actors, rebalancing the roles of users, platforms, and public authorities according to a vision of a rights-centric digital

society (European Commission, n.d.-e). Conversely, the US continues to grapple with the consequences of having granted private actors quasi-sovereign immunity in a regulatory vacuum designed to spur innovation, a choice made in the internet's infancy that has had profound and lasting consequences (Dickinson, 2024).

This article is guided by a primary research question: How do the regulatory philosophies, legal architectures, and enforcement mechanisms of the EU's Digital Services Act and the US's Section 230 differ in assigning responsibility for third-party content, and what are the implications of these differences for free expression, user safety, and platform innovation?

To answer this question, the analysis pursues four objectives. First, it will meticulously detail the legal framework of the DSA, examining its tiered due diligence obligations, liability model, and enforcement structure. Second, it will conduct a parallel examination of Section 230, tracing its legislative origins and its expansive judicial interpretation. Third, it will undertake a systematic comparative analysis, contrasting the core components of each regime and dissecting their underlying jurisprudential philosophies. Finally, it will assess their respective strengths, weaknesses, and future challenges, particularly in light of emerging technologies. The article proceeds in four subsequent parts: Part II analyses the EU's DSA; Part III examines the US's Section 230; Part IV conducts the comparative analysis; and Part V offers concluding reflections on the future of platform regulation. This analysis employs a comparative legal method, drawing on legislation, case law, policy papers, and scholarly articles to understand the underlying structures and cultural contexts of each legal system (Eberle, n.d.; Van Hoecke 2015).

2. THE EUROPEAN UNION'S PROACTIVE GOVERNANCE MODEL: THE DIGITAL SERVICES ACT

The Digital Services Act, formally Regulation (EU) 2022/2065, represents the most significant overhaul of the EU's legal framework for digital services in over two decades. It does not replace, but rather updates and builds upon, the foundational principles of the e-Commerce Directive 2000/31/EC, particularly its provisions on intermediary liability (Clifford Chance, 2022; William Fry, 2023.). The impetus for this modernisation was twofold. First, the digital landscape had transformed dramatically since 2000, with the rise of systemic platforms whose societal impact was unforeseen at the turn of the millennium (European Commission, n.d.-b). Second, the absence of a harmonised EU-level response to online harms had led to a fragmentation of the Digital Single Market, as Member States began enacting disparate national laws, most notably Germany's Network Enforcement Act (NetzDG). The DSA was conceived to remedy this fragmentation by establishing a single, uniform set of rules applicable across the Union (European Commission, n.d.-b; European Commission, n.d.-e).

The DSA is a cornerstone of the EU's broader digital strategy and operates in tandem with its sibling regulation, the Digital Markets Act (DMA) (European Commission, n.d.-d). While the DMA targets the economic power of designated 'gatekeeper' platforms to ensure fair and contestable markets, the DSA focuses on societal risks, aiming to create a "safer, predictable and trusted online environment" where the fundamental rights of users, as enshrined in the EU Charter, are effectively protected (European Commission, n.d.-e). This explicit grounding

in fundamental rights signals the EU's ambition to craft a form of digital constitutionalism, embedding public values into the architecture of private platforms.

A central innovation of the DSA is its asymmetric, tiered approach to regulation. It establishes a cumulative, four-layered system of due diligence obligations, where the stringency of the rules corresponds to the nature, size, and impact of the service provider (Clifford Chance, 2022; Protiviti, 2022; Roschier, n.d.).

All intermediary services, including basic 'mere conduit' and 'caching' services, are subject to a baseline set of obligations, such as establishing points of contact and providing transparency in their terms and conditions (Latham & Watkins, n.d.; Roschier, n.d.). The second tier applies to 'hosting services' (including online platforms), which must implement specific mechanisms for content moderation. The third tier adds further obligations for 'online platforms' (e.g., social networks, online marketplaces), such as internal complaint-handling systems and measures to protect minors. The fourth and most stringent tier applies exclusively to 'Very Large Online Platforms' (VLOPs) and 'Very Large Online Search Engines' (VLOSEs)—those with over 45 million monthly active users in the EU—which are deemed to pose systemic risks (European Commission, n.d.-a; Roschier, n.d.).

For all hosting services, Article 16 of the DSA mandates the implementation of a 'notice and action' mechanism (eu-digital-services-act.com, n.d.-a). This system must be easy to access and user-friendly, allowing any individual or entity to report content they consider to be illegal (Crowell & Moring LLP, 2024; eu-digital-services-act.com, n.d.-a). The notice must contain a sufficiently substantiated explanation for the allegation and a clear indication of the content's electronic location (eu-digital-services-act.com, n.d.-a). Upon receipt of such a notice, the provider must process it and make a decision „in a timely, diligent, non-arbitrary and objective manner” (eu-digital-services-act.com, n.d.-a). Crucially, for any content moderation decision taken—whether removal, demotion, or account suspension—the platform must provide the affected user with a clear and specific 'statement of reasons' (Deloitte, 2023; Zevo Health, 2024.). This proceduralisation of content moderation, coupled with rights to an internal appeal and out-of-court dispute settlement, aims to enhance due process and accountability for users whose expression is restricted (ACM, n.d.; Deloitte, 2023).

The most novel and far-reaching component of the DSA is its regulatory framework for VLOPs and VLOSEs. This framework moves beyond a reactive, content-by-content approach to a proactive, systems-based model of governance. Article 34 requires these large platforms to conduct, at least annually, a comprehensive risk assessment to identify, analyse, and assess systemic risks stemming from the design and functioning of their services (eu-digital-services-act.com, n.d.-c; Tech Policy Press, n.d.-a). These assessments must cover four broad categories of risk:

1. The dissemination of illegal content (eu-digital-services-act.com, n.d.-c).
2. Actual or foreseeable negative effects on the exercise of fundamental rights, including human dignity, privacy, and freedom of expression (eu-digital-services-act.com, n.d.-c).
3. Actual or foreseeable negative effects on civic discourse, electoral processes, and public security (eu-digital-services-act.com, n.d.-c).
4. Actual or foreseeable negative effects in relation to gender-based violence, the

protection of public health and minors, and serious negative consequences to a person's physical and mental well-being (eu-digital-services-act.com, n.d.-c; Sullivan, 2025).

When conducting these assessments, platforms must explicitly consider how their own systems—including their recommender algorithms, content moderation processes, and advertising models—influence these risks (eu-digital-services-act.com, n.d.-c). Following the assessment, Article 35 obliges VLOPs to put in place „reasonable, proportionate and effective” mitigation measures tailored to the specific risks identified (European Parliament Think Tank, 2025; Efroni, 2021). These measures are not prescribed but may include adapting recommender systems, reinforcing internal processes, or initiating cooperation under codes of conduct (European Parliament Think Tank, 2025; Tech Policy Press, n.d.-a). The entire risk management cycle—from assessment to mitigation—is subject to an annual independent audit, the results of which must be submitted to regulators (European Parliament Think Tank, 2025; Tech Policy Press, n.d.-a). This framework represents a fundamental shift in regulatory philosophy, moving the focus from policing individual pieces of content to scrutinising the underlying platform architectures that amplify and disseminate such content at scale. It treats platforms not as neutral hosts but as complex socio-technical systems whose design choices have foreseeable and regulatable societal consequences.

The DSA preserves the core liability exemption, or ‘safe harbour’, established by the e-Commerce Directive (Clifford Chance, 2022; Latham & Watkins, n.d.). Under this principle, hosting service providers are not liable for illegal information stored at the request of a user, provided that the provider: (a) does not have actual knowledge of the illegal activity or information; and (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the information (Latham & Watkins, n.d.; Scheurman, 2022). The DSA clarifies that providers do not lose this exemption simply because they undertake voluntary own-initiative investigations to detect illegal content (Latham & Watkins, n.d.).

However, the DSA recalibrates this liability shield by making it implicitly conditional upon compliance with the new due diligence obligations. While the regulation does not create a general monitoring obligation, a failure to implement and properly operate the mandated notice-and-action mechanism, or to act upon a sufficiently precise notice that would give a diligent provider actual knowledge of illegality, could lead a court to find that the conditions for the safe harbour are no longer met (Crowell & Moring LLP, 2024). This creates a powerful incentive for procedural compliance, as the liability shield is no longer a passive protection but one that must be actively maintained through diligent process.

The DSA establishes a novel, dual-layered enforcement structure to ensure its application across the Union (European Commission, n.d.-a). At the national level, each Member State must designate a Digital Services Coordinator (DSC), an independent authority responsible for supervising the intermediary services established in its territory (European Commission, 2025a; European Commission, n.d.-f). DSCs are endowed with significant investigative and enforcement powers, including the ability to request information, conduct inspections, and impose fines (Department of Enterprise, Trade and Employment, 2024; eu-digital-services-act.com, n.d.-d). They also play a crucial role in the broader ecosystem by certifying ‘trusted flaggers’ and out-of-court dispute settlement bodies (European Commission, 2025a).

At the EU level, the European Commission has exclusive competence to supervise and

enforce the specific obligations for VLOPs and VLOSEs related to mitigating systemic risks (European Commission, 2025a; European Commission, n.d.-a). To ensure consistent application of the DSA, the national DSCs form a new independent advisory group, the European Board for Digital Services, which is chaired by the Commission (eu-digital-services-act.com, n.d.-e; European Commission, 2024). This structure is backed by a formidable sanctions regime. Non-compliance with the DSA can result in fines of up to 6% of a company's global annual turnover, with periodic penalties of up to 5% of average daily turnover for ongoing infringements (European Commission, 2025b; Protiviti, 2022). This financial leverage is designed to ensure that even the largest global platforms take their new obligations seriously (Granick 2023).

Since the DSA's obligations for VLOPs took effect in August 2023, its implementation has been marked by both platform adaptation and significant contestation. Several platforms have updated their services to comply; for example, YouTube has enhanced its 'Trusted Flagger' program and expanded its transparency reporting (Google, 2023). However, the new framework has also been met with legal and political resistance. Meta has launched legal challenges against the supervisory fees levied by the Commission to fund DSA enforcement, calling the calculation method „opaque” and „absurd” (Marketing Tech News, 2025a, 2025b). Furthermore, Meta's recent changes to its content moderation policies in the US, which relax standards on hate speech and move away from third-party fact-checking, have created significant tension with its systemic risk mitigation duties under the DSA in Europe (Counter Hate, 2025; European Parliament Think Tank, 2025; Morningstar, n.d.; TechPolicy. Press, n.d.-b).

The most prominent early test case for DSA enforcement involves X (formerly Twitter). In December 2023, the European Commission opened its first formal infringement proceedings against the platform, investigating potential breaches related to the dissemination of illegal content, the effectiveness of its 'Community Notes' system, advertising transparency, and deceptive design features ('dark patterns') associated with its subscription services (eucrim, 2023; Tech Policy Press, n.d.-c). Preliminary findings have since indicated that X is in Pingen of its obligations regarding its ad repository and data access for researchers (Werner, 2024; Tech Policy Press, n.d.-d). These high-profile enforcement actions signal the Commission's intent to vigorously enforce the DSA's provisions and establish its credibility as a powerful digital regulator.

3. THE UNITED STATES' ENDURING IMMUNITY DOCTRINE: SECTION 230 OF THE COMMUNICATIONS DECENCY ACT

Section 230 of the Communications Decency Act of 1996 is a product of the nascent internet era, drafted to address a specific legal conundrum that threatened the growth of online services (Dickinson, 2024; Electronic Frontier Foundation, n.d.-a; Wake Forest Law Review, n.d.). In the early 1990s, US courts, applying traditional common law principles of defamation, produced two conflicting precedents. In *Cubby, Inc. v. CompuServe, Inc.* (1991), a court found that an online service provider that exercised no editorial control over user content was akin to a distributor (like a newsstand) and could not be held liable for defamatory material without knowledge of its existence (Electronic Frontier Foundation,

n.d.-a; Harvard Law Review, 2018). Conversely, in *Stratton Oakmont, Inc. v. Prodigy Servs. Co.* (1995), a court held that because Prodigy actively moderated content to enforce its guidelines, it had assumed the role of a traditional publisher and could therefore be held liable for all defamatory statements on its service (Electronic Frontier Foundation, n.d.-a).

This created what became known as the ‘moderator’s dilemma’: an online service could either refrain from any moderation and risk becoming a cesspool of harmful content, or attempt to moderate and thereby incur publisher liability for any content that slipped through its filters (Electronic Frontier Foundation, n.d.-a; EPIC, 2025). Congress enacted Section 230 as a direct response to this dilemma. Its dual purpose was to immunise platforms from liability for third-party content, thereby encouraging them to host user speech, while simultaneously encouraging them to voluntarily moderate „obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable” material without fear that such actions would create liability (Communications Decency Act, 1996, 47 U.S.C. § 230; Electronic Frontier Foundation, n.d.-a).

The core of Section 230’s immunity is found in the 26 words of subsection (c)(1): „No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider” (Communications Decency Act, 1996, 47 U.S.C. § 230; Wake Forest Law Review, n.d.). While the text itself is concise, its power lies in the broad interpretation it has received from the judiciary over the past quarter-century.

The cornerstone of this expansive interpretation is the 1997 decision of the Fourth Circuit Court of Appeals in *Zeran v. America Online, Inc.* (Electronic Frontier Foundation, 1997). The case involved a malicious hoax where an anonymous user posted advertisements for offensive T-shirts related to the Oklahoma City bombing, listing the plaintiff’s personal phone number (First Amendment Encyclopedia, 1997; Electronic Frontier Foundation, 1997). Despite being notified by the plaintiff, AOL failed to promptly remove all postings. The plaintiff sued, arguing that once AOL had notice of the defamatory content, it had a duty as a distributor to remove it (Electronic Frontier Foundation, 1997).

The Fourth Circuit rejected this argument, delivering a sweeping interpretation of Section 230. The court held that the statute created a broad federal immunity that pre-empted any state-law cause of action that would treat a service provider as a publisher, including claims of distributor liability (Electronic Frontier Foundation, 1997). It reasoned that imposing liability upon notice would force platforms into the very publisher role that Congress sought to avoid, creating a chilling effect on speech and disincentivising moderation (Electronic Frontier Foundation, 1997). The *Zeran* decision established that Section 230 provides near-absolute immunity for platforms regarding third-party content, a precedent that has been almost uniformly followed by US courts and has become the bedrock of the modern internet’s legal architecture (First Amendment Encyclopedia, 1997; Goldman & Kosseff 2017.).

For decades, the *Zeran* precedent remained largely unchallenged. However, the technological evolution of platforms from passive hosts to active curators of content via sophisticated algorithms raised new questions about the scope of Section 230’s immunity. The central issue became whether a platform’s algorithmic recommendation of harmful content constitutes its own speech, thereby falling outside the protection for information

„provided by another” (Moss, 2023). This question reached the US Supreme Court in 2023 in *Gonzalez v. Google, LLC* (U.S. Supreme Court 2022; SCOTUSblog, 2025). The plaintiffs, family members of a victim of an ISIS terrorist attack, argued that YouTube (owned by Google) aided and abetted terrorism by using its algorithms to recommend ISIS videos to users (U.S. Supreme Court 2022; Moss, 2023).

The case was widely seen as a potential vehicle for the Supreme Court to clarify or narrow the scope of Section 230 for the modern era (Nagle & Hogan, 2019; Wake Forest Law Review, n.d.). However, in a brief, unsigned opinion, the Court declined to address the Section 230 question at all (Covington & Burling LLP, 2023). Instead, it resolved the case by referring to its companion decision in *Twitter, Inc. v. Taamneh*, where it found that the platforms’ generalised services did not amount to „aiding and abetting” terrorism under the relevant statute (Covington & Burling LLP, 2023; Global Freedom of Expression, Columbia University, 2023). By „punting” on the central issue, the Supreme Court left the critical legal question of liability for algorithmic amplification unresolved, leaving the expansive *Zeran*-era interpretation intact but under a cloud of uncertainty (Covington & Burling LLP, 2023; Harvard Kennedy School, 2018). This judicial reluctance highlights a deep institutional discomfort with reconciling a legal framework designed for the 1996 internet of bulletin boards with the 2023 technological reality of algorithmically-driven platforms (Wake Forest Law Review, n.d.). The law remains dependent on the legal fiction that platforms are not publishers, a fiction increasingly strained by the fact that their core business model is the algorithmic curation and promotion of content—an inherently editorial function.

Section 230’s legacy is deeply contested. Its proponents credit it with enabling the explosive growth and innovation of the digital economy, protecting a vast range of online speech, and providing the legal foundation for the rise of user-generated content platforms and social movements like #MeToo and Black Lives Matter (ACLU, 2023; Electronic Frontier Foundation, 2025; McCain Institute, n.d.). From this perspective, the immunity is a vital bulwark for free expression, preventing platforms from engaging in excessive, risk-verse censorship.

Conversely, critics from across the political spectrum argue that the broad immunity has created a moral hazard, shielding multi-billion-dollar corporations from accountability for the immense social costs their platforms generate (Armijo, 2021.; McMahon & Narayan, 2023.). This critique holds that Section 230 allows platforms to profit from engagement-driven models that amplify harmful content—such as disinformation, hate speech, harassment, and extremist material—while externalising the costs of these harms onto society (Moss, 2023.; Overton & Powell, 2024).

The growing criticism of Section 230 has led to a flurry of legislative reform proposals in recent years, though no consensus has emerged (Verveer, 2023). The debate is highly politicised, with different factions seeking reform for contradictory reasons. Some proposals, including those from the Department of Justice under the Trump administration, have focused on creating carve-outs to the immunity for particularly egregious harms, such as child sexual abuse material, terrorism, and cyber-stalking (U.S. Department of Justice, 2020). Other proposals seek to condition the liability shield on platforms adhering to certain standards of procedural fairness or „politically neutral” content moderation, a response to

claims of anti-conservative bias (Congressional Research Service, n.d.-a; Armijo, 2021).

These reform efforts face significant hurdles, not least the First Amendment, which protects the editorial discretion of private platforms and limits the government's ability to compel or prohibit certain types of content moderation (Congressional Research Service, n.d.-a; Armijo, 2021.). Furthermore, the rapid emergence of generative AI is introducing a new layer of complexity. AI systems that generate novel content by synthesising vast datasets blur the line between a platform providing a neutral tool and being a creator of content itself, posing a direct challenge to Section 230's foundational distinction between an „interactive computer service” and an „information content provider” (Gray & Block, 2024; Congressional Research Service, n.d.-b; Crowell & Moring LLP, 2025.; Public Knowledge, n.d.)

4. A COMPARATIVE JURISPRUDENCE OF PLATFORM LIABILITY

A direct comparison of the DSA and Section 230 reveals two fundamentally different regulatory architectures. The DSA's scope is extraterritorial and comprehensive, applying to any intermediary service offered to users located in the EU, with obligations tiered according to the service's function and size (European Commission, n.d.-e; Latham & Watkins, n.d.). Section 230, by contrast, applies to „interactive computer services” within US jurisdiction, a broad but domestically focused category (Congressional Research Service, n.d.-a; Dickinson, 2024).

The most profound difference lies in their approach to platform duties. The DSA is a regime of affirmative obligations. It imposes a detailed set of mandatory due diligence requirements, including transparency reporting, proceduralised notice-and-action systems, and, for VLOPs, proactive risk assessments and mitigation (European Commission, 2020; Roschier, n.d.). Section 230 imposes no affirmative duties. It is a purely defensive statute, providing a legal shield against liability but not compelling platforms to take any specific action to moderate content or protect users (Communications Decency Act, 1996, 47 U.S.C. § 230; Scheurman, 2022).

This divergence extends to their enforcement models. The DSA establishes a powerful, state-led administrative regime, with national DSCs and the European Commission actively supervising platforms and imposing severe financial penalties for non-compliance (European Commission, 2025b; European Commission, n.d.-a). Section 230, on the other hand, is enforced passively through the judiciary. It functions as a defence invoked by platforms in private civil litigation to secure the dismissal of lawsuits (Congressional Research Service, n.d.-a).

These architectural differences are rooted in deeply divergent jurisprudential philosophies. The DSA is a clear expression of what scholars have termed European 'digital constitutionalism' (Lasa 2024.; De Gregorio 2022). This philosophy seeks to project public law values—such as the protection of fundamental rights, human dignity, consumer safety, and democratic oversight—onto the powerful private actors that govern digital spaces (epicenter.works, 2019). It is a proactive, interventionist model that views the state as having a positive obligation to structure the digital environment to be conducive to these values.

Section 230 is a product of the quintessentially American ‘marketplace of ideas’ tradition, which is heavily influenced by a negative-liberty interpretation of the First Amendment (epicenter.works, 2019; De Gregorio, 2022). This philosophy posits that the best way to arrive at truth is through the robust and largely unregulated competition of speech in the public square (De Gregorio, 2022). It is deeply sceptical of state intervention, prioritising the unfettered flow of information and market-led innovation over state-mandated safety or content standards. The law’s purpose was to allow this marketplace to flourish online with minimal government or judicial interference.

Each model possesses distinct strengths and weaknesses. The primary strength of Section 230’s broad immunity has been its undeniable success in fostering innovation and protecting a wide spectrum of online expression, creating the dynamic and participatory internet of the last two decades (Electronic Frontier Foundation, 2025; Electronic Frontier Foundation, n.d.-b). Its principal weakness is the profound lack of accountability for the systemic harms and negative externalities that this unregulated environment has produced (Moss, 2023.; McMahon, K., & Narayan, 2023.).

The DSA’s strengths lie in its comprehensive attempt to create a harmonised and accountable regulatory environment that prioritises user rights and safety (Planet Compliance, n.d.; TrustArc, n.d.). Its potential weaknesses include the risk of high compliance costs, particularly for smaller platforms, the potential for over-regulation to stifle innovation, and the danger that aggressive enforcement could lead to a chilling of legitimate speech as platforms become overly cautious to avoid sanctions (Broadbent, 2020; Protiviti, 2022; TechReg, n.d.). The two frameworks thus represent a classic trade-off between innovation and accountability, freedom and safety.

The following table synthesises the key differences between the two regulatory regimes.

Table 1. Comparative Analysis Matrix

Feature	EU Digital Services Act (DSA)	US Section 230 CDA
Regulatory Philosophy	Digital Constitutionalism: Proactive, risk-based regulation to protect fundamental rights and user safety.	Marketplace of Ideas: Reactive immunity to foster innovation and protect free expression from liability.
Primary Goal	Create a safe, predictable, and trusted online environment; harmonise the digital single market.	Promote the development of the internet unfettered by regulation; encourage voluntary content moderation.
Scope of Application	Tiered obligations for all "intermediary services" offered to users in the EU, regardless of establishment.	"Interactive computer services" and their "users" within US jurisdiction.
Liability Standard	Conditional Safe Harbour: Immunity from liability for third-party content is conditional on compliance with procedural due diligence obligations.	Broad Immunity: Near-absolute immunity from being treated as the "publisher or speaker" of third-party content.
Core Obligations	Affirmative Duties: Mandatory due diligence, transparency reports, notice-and-action systems, risk assessments for VLOPs.	No Affirmative Duties: Provides a legal shield (an immunity defence) but imposes no obligations to moderate or act.

Feature	EU Digital Services Act (DSA)	US Section 230 CDA
Content Moderation	Proceduralised: Mandates notice-and-action, statements of reason, internal complaint systems, and out-of-court dispute settlement.	Discretionary: Platforms have broad discretion under the "Good Samaritan" clause (230(c)(2)) to remove content they deem "objectionable."
Algorithmic Systems	Regulated: Requires transparency on recommender systems; VLOPs must assess and mitigate systemic risks from algorithms.	Largely Unresolved: Gonzalez v. Google left the question of liability for algorithmic amplification unanswered.
Advertising	Regulated: Requires transparency for all ads; bans targeted ads to minors and those based on sensitive data.	Largely Unregulated: Immunity generally applies, though some claims for discriminatory ad targeting have survived.
Enforcement Body	Administrative/State-led: European Commission (for VLOPs) and national Digital Services Coordinators.	Judicial/Private-led: Enforced by courts as a defence in civil litigation.
Sanctions/Remedies	Severe Penalties: Fines up to 6% of global annual turnover; periodic penalties; temporary suspension of service.	Dismissal of Lawsuit: The primary remedy is the dismissal of the civil claim against the platform.

Source: created by the author.

The structural coherence within each column of the matrix is revealing. In the EU, the philosophy of digital constitutionalism logically leads to proactive duties, proceduralised moderation, and state-led administrative enforcement. In the US, the marketplace of ideas philosophy logically produces a reactive immunity shield, discretionary moderation, and judicial enforcement through private litigation. This deep coherence underscores that the two regimes are not merely different sets of rules but are entirely distinct, self-contained legal paradigms. They are predicated on conflicting theories of harm: the DSA operates on a theory of systemic risk, where the harm emanates from the platform's very design and operation (eu-digital-services-act.com, n.d.-c), while Section 230 operates on a theory of individual tort, where the harm emanates from a specific piece of content created by a user (Electronic Frontier Foundation, 1997). This fundamental incompatibility in how the problem is defined makes any simple convergence or harmonisation between the two models highly improbable.

5.CONCLUSION: PATHWAYS TO A MORE RESPONSIBLE DIGITAL FUTURE

This analysis has demonstrated that the European Union and the United States have embarked on starkly divergent paths in regulating online platform liability. The EU's Digital Services Act has established a proactive, comprehensive, and rights-based regulatory model that imposes significant affirmative duties on platforms, particularly the largest ones, to assess and mitigate systemic risks. It is a system of conditional liability enforced by a powerful administrative apparatus. The US's Section 230, as interpreted by its judiciary, remains a reactive, speech-protective immunity doctrine that provides a broad shield from liability with no corresponding affirmative obligations, enforced primarily as a defence in private litigation.

The practical implications of this transatlantic divide are profound. Global platforms must

now operate within a bifurcated regulatory landscape, facing complex compliance challenges that may lead them to geo-fence certain features or adopt the stricter EU standards globally to ensure operational consistency (Counter Hate, 2025; Morningstar, n.d.). For users, the divergence creates a tale of two internets: one within the EU, where users are endowed with greater procedural rights, transparency, and avenues for redress; and one in the US, where users' experiences are largely subject to the discretionary governance of platform operators. For regulators, the DSA provides a powerful new toolkit for oversight, while US legislators and regulators remain mired in a political deadlock over potential reforms.

While direct adoption of the DSA in the US is politically and constitutionally implausible, the potential for indirect convergence exists. The DSA may exert a 'Brussels Effect', setting a global de facto standard for responsible platform governance that US-based companies adopt worldwide to simplify their compliance architecture and mitigate reputational risk (Reddit, n.d.). Certain concepts from the DSA, such as enhanced transparency in content moderation and advertising, or greater user control over recommender systems, could also inform more modest, politically viable reforms to Section 230 in the future. However, the fundamental philosophical and structural differences identified in this analysis suggest that a deep harmonisation of the two regimes is not on the horizon.

The ultimate long-term impact of the DSA may extend beyond its specific rules to its creation of a permanent, institutionalised capacity for regulatory oversight within the EU. Through the Commission's dedicated enforcement teams, the network of national DSCs, the European Board for Digital Services, and knowledge-generating bodies like the European Centre for Algorithmic Transparency (ECAT), the EU is building a sophisticated bureaucratic and expert infrastructure designed for the continuous monitoring and regulation of complex digital systems (European Commission, 2024; European Commission, 2025a; White & Case, 2025). The United States, by contrast, lacks any comparable institutional capacity, leaving oversight fragmented and reform dependent on a gridlocked legislative process (Harvard Kennedy School, 2018; U.S. Department of Justice, 2020). This emerging 'capacity gap' suggests that the transatlantic divergence is not merely legal but deeply institutional, and is likely to widen over time.

Both models will be severely tested by the next wave of technological change. The rise of generative AI, which blurs the line between a platform as a conduit and a creator, directly challenges the core legal distinction upon which Section 230 is built (Congressional Research Service, n.d.-b; Gray & Block, 2024.). Similarly, the emergence of decentralised platforms and the metaverse will create novel governance challenges that may not fit neatly into either the DSA's centralised enforcement model or Section 230's intermediary-focused framework (Number Analytics, 2025). While the EU and the US have chosen profoundly different paths today, the relentless pace of technological evolution will force both to continually re-evaluate and adapt their approaches to the enduring challenge of balancing innovation with responsibility in the digital age.

REFERENCES

- 47 U.S.C. § 230 (2024). Protection for private blocking and screening of offensive material. Cornell Law School, Legal Information Institute. <https://www.law.cornell.edu/uscode/text/47/230>
- ACM. (n.d.). Guidelines on DSA due diligence obligations for intermediary services. Retrieved from <https://www.acm.nl/system/files/documents/guidelines-dsa-due-diligence-obligations-for-intermediary-services.pdf>
- Armijo, E. (2021). Reasonableness as censorship: Section 230 reform, content moderation, and the First Amendment. *Florida Law Review*, 73(6), 1199–1249. <https://scholarship.law.ufl.edu/flr/vol73/iss6/2>
- Broadbent, M. (2020, November 10). The Digital Services Act, the Digital Markets Act, and the new competition tool: European initiatives to hobble U.S. tech companies. Center for Strategic and International Studies. <https://www.csis.org/analysis/digital-services-act-digital-markets-act-and-new-competition-tool>
- Clifford Chance. (2022). The Digital Services Act: What is it and what impact will it have? Retrieved from <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/12/the-digital-services-act-what-is-it-and-what-impact-will-it-have-updated-december-2022.pdf>
- Congressional Research Service. (2023). Generative Artificial Intelligence and Section 230. Retrieved from <https://www.congress.gov/crs-product/LSB11097>
- Congressional Research Service. (2024). Section 230: An Overview. Retrieved from <https://www.congress.gov/crs-product/R46751>
- Counter Hate. (2025). How will Meta's policy changes affect European users? Retrieved from <https://counterhate.com/blog/how-will-metas-policy-changes-affect-european-users/>
- Covington & Burling LLP. (2023). The US Supreme Court punts on Section 230 in *Gonzalez v. Google LLC*. Retrieved from <https://www.cov.com/en/news-and-insights/insights/2023/05/the-us-supreme-court-punts-on-section-230-in-gonzalez-v-google-llc>
- Crowell & Moring LLP. (2024). Notice and action mechanisms in the DSA: Balancing the removal of illegal content and the freedom of expression. Retrieved from <https://www.crowell.com/en/insights/client-alerts/notice-and-action-mechanisms-in-the-dsa-balancing-the-removal-of-illegal-content-and-the-freedom-of-expression>
- Crowell & Moring LLP. (2025). Section 230 Reform: What Websites Need to Know Now. Retrieved from <https://www.crowell.com/en/insights/client-alerts/section-230-reform-what-websites-need-to-know-now>
- De Gregorio, G. (2022). Digital constitutionalism across the Atlantic. *Global Constitutionalism*, 11(2), 297–324. doi:10.1017/S2045381722000016
- Deloitte. (2023). Legal implications of the Digital Services Act. Retrieved from <https://www.deloitte.com/nl/en/services/legal/perspectives/legal-implications-of-the-digital-services-act.html>
- Department of Enterprise, Trade and Employment. (2024). Digital Services Act. Retrieved from <https://enterprise.gov.ie/en/what-we-do/the-business-environment/digital-single-market/eu-digital-single-market-aspects/digital-services-act/>
- Dickinson, G. M. (2024). A Juridical History of Section 230. *Stanford Technology Law Review*, 28(1). Retrieved from <https://law.stanford.edu/wp-content/uploads/2025/02/A-Juridical-History-of-Section-230.pdf>
- Dothan, S. (2014). The optimal use of comparative law. *Denver Journal of International Law & Policy*, 43(1), 21–44.
- Eberle, E. J. (2011.). The methodology of comparative law. *Roger Williams University Law Review*, 16(1). https://docs.rwu.edu/cgi/viewcontent.cgi?article=1445&context=rwu_LR
- Efroni, Z. (2021, Nov 16). The Digital Services Act: risk-based regulation of online platforms. *Internet Policy Review*. <https://policyreview.info/articles/news/digital-services-act-risk-based-regulation-online-platforms/1606>
- Electronic Frontier Foundation. (1997). *Zeran v. America Online, Inc.* Retrieved from <https://www.eff.org/files/zeran-v-aol.pdf>
- Electronic Frontier Foundation. (2025). Section 230. Retrieved from <https://www.eff.org/issues/cda230>
- Electronic Frontier Foundation. (n.d.-a). CDA 230: Legislative history. Retrieved from <https://www.eff.org/issues/cda230/legislative-history>
- Electronic Frontier Foundation. (n.d.-b). Section 230: The law that gives us the modern internet. Retrieved from <https://www.eff.org/issues/cda230>
- EPIC. (2025). *California et al. v. Meta, Inc. et al.* Retrieved from <https://epic.org/documents/california-et-al-v-meta-inc-et-al/>

- epicenter.works. (2019). EU vs USA: What can different attitudes towards platform regulation teach us? Retrieved from <https://epicenter.works/en/content/eu-vs-usa-what-can-different-attitudes-towards-platform-regulation-teach-us>
- eu-digital-services-act.com. (n.d.-a). Article 16, Notice and action mechanisms - the Digital Services Act (DSA). Retrieved from https://www.eu-digital-services-act.com/Digital_Services_Act_Article_16.html
- eu-digital-services-act.com. (n.d.-b). Digital Services Act Preamble 111-120. Retrieved from https://www.eu-digital-services-act.com/Digital_Services_Act_Preamble_111_to_120.html
- eu-digital-services-act.com. (n.d.-c). Digital Services Act Article 34. Retrieved from https://www.eu-digital-services-act.com/Digital_Services_Act_Article_34.html
- eu-digital-services-act.com. (n.d.-d). Digital Services Act Article 61. Retrieved from https://www.eu-digital-services-act.com/Digital_Services_Act_Article_61.html
- European Commission. (2020). Questions and Answers: Digital Services Act. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348
- European Commission. (2024). European Board for Digital Services. Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/dsa-board>
- European Commission. (2025a). Digital Services Coordinators. Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs>
- European Commission. (2025b). The enforcement framework under the Digital Services Act. Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement>
- European Commission. (n.d.-a). The Digital Services Act. Retrieved from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en
- European Commission. (n.d.-b). Digital Services Act (DSA) Preamble 1-10. Retrieved from https://www.eu-digital-services-act.com/Digital_Services_Act_Preamble_1_to_10.html
- European Commission. (n.d.-c). The Digital Services Act package. Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>
- European Commission. (n.d.-d). The Digital Services Act package. Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>
- European Commission. (n.d.-e). The Digital Services Act package. Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>
- European Commission. (n.d.-f). Digital Services Coordinators. Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs>
- European Parliament Think Tank. (2025). Fact-checking and content moderation. Retrieved from <https://epthinktank.eu/2025/02/19/fact-checking-and-content-moderation/>
- First Amendment Encyclopedia. (1997). *Zeran v. America Online, Inc.* (4th Cir.). Retrieved from <https://firstamendment.mtsu.edu/article/zeran-v-america-online-inc-4th-cir/>
- Global Freedom of Expression, Columbia University. (2023). *Gonzalez v. Google* (SCOTUS, 2023). Retrieved from <https://globalfreedomofexpression.columbia.edu/cases/gonzalez-v-google-scotus-2023/>
- Goldman, E., & Kosseff, J. (2017, November 10). Commemorating the 20th anniversary of Internet law's most important judicial decision. In *Zeran v. AOL: 20th Anniversary Essays*. Retrieved from <https://www.roschier.com/newsroom/four-layers-of-due-diligence-in-the-eu-digital-services-act>
- Google. (2023). Complying with the Digital Services Act. Retrieved from <https://blog.google/around-the-globe/google-europe/complying-with-the-digital-services-act/>
- Granick, J. S. (2023). Is this the end of the Internet as we know it? American Civil Liberties Union. <https://www.aclu.org/news/free-speech/section-230-is-this-the-end-of-the-internet-as-we-know-it>
- Gray, J., & Block, A. (2024, November 14). Beyond the search bar: Generative AI's Section 230 tightrope walk. American Bar Association. Retrieved from: https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-november/beyond-search-bar-generative-ai-section-230-tightrope-walk/
- Harvard Law Review. (2018). Section 230 as First Amendment Rule. Retrieved from https://harvardlawreview.org/wp-content/uploads/2018/05/2027-2048_Online.pdf
- Lasa, A. (2024). The systematics of the European Artificial Intelligence Act in the context of the fundamental rights of the Union: The myth of the digital constitutionalism. *Deusto Journal of Human Rights*, 14, 73–100. <https://doi.org/10.18543/djhr.3189>
- Latham & Watkins. (n.d.). Digital Services Act: Practical Implications for Online Services and Platforms. Retrieved from <https://www.lw.com/admin/upload/SiteAttachments/Digital-Services-Act-Practical->

Implications-for-Online-Services-and-Platforms.pdf

Liberties. (2025). Monitoring the implementation of the Digital Services Act. Retrieved from https://dq4n3btxmr8c9.cloudfront.net/files/0ol1bo/Liberties_DSA_Monitoring_Febr2025.pdf

Marketing Tech News. (2025a). Meta Platforms has challenged the Digital Services Act (DSA) fees. Retrieved from <https://www.marketingtechnews.net/news/digital-services-act-fees-meta-tiktok-challenge/>

Marketing Tech News. (2025b). Meta and TikTok slams Digital Services Act fees as 'absurd' and 'discriminatory'. Retrieved from <https://www.marketingtechnews.net/news/digital-services-act-fees-meta-tiktok-challenge/>

McCain Institute. (2023). Section 230 and Disinformation. Retrieved from <https://www.mccaininstitute.org/resources/blog/section-230-and-disinformation/>

McMahon, K., & Narayan, A. (2023). Uproot or upgrade? Revisiting Section 230 immunity in the digital age. University of Chicago Law Review Online. <https://lawreview.uchicago.edu/online-archive/uproot-or-upgrade-revisiting-section-230-immunity-digital-age>

Morningstar. (2025). Why Meta's new content moderation policy could pose risks to its stock. Retrieved from <https://global.morningstar.com/en-gb/sustainable-investing/why-metas-new-content-moderation-policy-could-pose-risks-its-stock>

Moss, R. (2023, July 21). The future of Section 230: What does it mean for consumers? National Association of Attorneys General. <https://www.naag.org/consumer-protection/the-future-of-section-230-what-does-it-mean-for-consumers/>

Nagle, J., & Hogan, M. (2019). What can we learn about rising inequality? Archived working paper no. 197. Harvard Kennedy School, Mossavar-Rahmani Center for Business and Government. /mnt/data/197_AWP_final.pdf

Number Analytics. (2025). The Future of Free Speech. Retrieved from <https://www.numberanalytics.com/blog/future-of-free-speech>

Olakoyenikan, O. (2024). Legal and ethical implications of misinformation: A comparative study of regulatory approaches in the European Union and the United States. *International Journal of Advanced Mass Communication and Journalism*, 5(2), 21–26. <https://www.masscomjournal.com/article/82/5-2-4-469.pdf>

Overton, S. A., & Powell, C. (2024). The Implications of Section 230 for Black communities. GWU. Retrieved from https://scholarship.law.gwu.edu/faculty_publications/1756/

Pingen, A. (2023). First formal proceedings launched by Commission under DSA: X under investigation. *eucrim – European Criminal Law Review*, 3, 245–246. (Published online 18 January 2024). <https://eucrim.eu/news/first-formal-proceedings-launched-by-commission-under-dsa-x-under-investigation/>

Planet Compliance. (2024). Digital Services Act. Retrieved from <https://www.planetcompliance.com/news/digital-services-act/>

Protiviti. (2022). Digital Services Act. Retrieved from https://www.protiviti.com/sites/default/files/2022-12/protiviti-white_paper-digital-services-act-TMT-GLOBAL.pdf

Public Knowledge. (2025). Public Knowledge Proposes Section 230 Reforms That Address Harms While Protecting Free Expression. Retrieved from <https://publicknowledge.org/public-knowledge-proposes-section-230-reforms-that-address-harms-while-protecting-free-expression/>

Roschier. (2024). Four Layers of Due Diligence in the EU Digital Services Act. Retrieved from <https://www.roschier.com/newsroom/four-layers-of-due-diligence-in-the-eu-digital-services-act>

Scheurman, T. (2022). Comparing Social Media Content Regulation in the US and the EU: How the US Can Move Forward With Section 230 to Bolster Social Media Users' Freedom of Expression. *San Diego International Law Journal*, 23(2), 413. Retrieved from <https://digital.sandiego.edu/ilj/vol23/iss2/5/>

SCOTUSblog. (2025). *Gonzalez v. Google LLC*. Retrieved from <https://www.scotusblog.com/cases/case-files/gonzalez-v-google-llc/>

Sullivan, D. (2025). Systemic Risk Assessments Hold Clues for EU Platform Enforcement. *Lawfare*. Retrieved from <https://www.lawfaremedia.org/article/systemic-risk-assessments-hold-clues-for-eu-platform-enforcement>

Tech Policy Press. (2023). Assessing Systemic Risk Under the Digital Services Act. Retrieved from <https://www.techpolicy.press/assessing-systemic-risk-under-the-digital-services-act/>

Tech Policy Press. (2024). Elon Musk's X breaches EU law over blue checkmark, ad transparency. Retrieved from <https://www.techpolicy.press/elon-musks-x-breaches-eu-law-over-blue-checkmark-ad-transparency/>

Tech Policy Press. (2025a). Meta's Content Moderation Changes are Going to Have a Real World Impact. It's Not Going to be Good. Retrieved from <https://www.techpolicy.press/metas-content-moderation-changes-are-going-to-have-a-real-world-impact-its-not-going-to-be-good/>

- Tech Policy Press. (2025b). Understanding the EU's Digital Services Act enforcement against X. Retrieved from <https://www.techpolicy.press/understanding-the-eus-digital-services-act-enforcement-against-x/>
- TechReg. (n.d.). The role of codes in the DSA. Retrieved from <https://techreg.org/article/view/18139>
- TrustArc. (n.d.). Digital Services Act. Retrieved from <https://trustarc.com/resource/digital-services-act/>
- U.S. Department of Justice. (2020). Department of Justice's review of Section 230 of the Communications Decency Act of 1996. Retrieved from <https://www.justice.gov/archives/ag/departments-justice-s-review-section-230-communications-decency-act-1996>
- U.S. Supreme Court. (2022). Gonzalez v. Google LLC (Docket No. 21-1333). Legal Information Institute, Cornell Law School. <https://www.law.cornell.edu/supct/cert/21-1333>
- Van Hoecke, M. (2015). Methodology of Comparative Legal Research. Law and Method, <https://doi.org/10.5553/REM/.000010>
- Verveer, P. L. (2023). Content moderation in the United States and Europe: Similar values, different approaches (M-RCBG Associate Working Paper Series, No. 197). Harvard Kennedy School, Mossavar-Rahmani Center for Business and Government. Retrieved from https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/197_AWP_final.pdf
- Werner, J. (2024, December 7). EU Commission identifies preliminary breaches of Digital Services Act by X (formerly Twitter). BABL AI. Retrieved from: <https://babl.ai/eu-commission-identifies-preliminary-breaches-of-digital-services-act-by-x-formerly-twitter/>
- White & Case. (2025). European Commission Publishes DSA Elections Toolkit to Support Digital Services Coordinators. Retrieved from <https://www.whitecase.com/insight-alert/european-commission-publishes-dsa-elections-toolkit-support-digital-services>
- William Fry. (2023). The Digital Service Act: Overview and Key Obligations. Retrieved from <https://www.williamfry.com/knowledge/the-digital-service-act-overview-and-key-obligations/>
- Zevo Health. (2024). Preparing for 2025: New regulations and their impact on content moderation and moderator wellbeing. Retrieved from <https://www.zevohealth.com/blog/preparing-for-2025-new-regulations-and-their-impact-on-content-moderation-and-moderator-wellbeing/>