INTERNET POLICY REVIEW

Volume 15 **Issue** 4

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Strategic compliance narratives: Platform governance under the DMA and DSA

Linda Weigl *University of Amsterdam* l.weigl@uva.nl

DOI: https://doi.org/10.14763/2026.4.2129

Published: 22 October 2026
Received: 24 June 2026 **Accepted:** 4 September 2026

Funding: This publication has been supported via the UvA Trust in the digital society RPA
Competing Interests: The author has declared that no competing interests exist that have influenced the text.
Licence: This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 License (Germany) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. https://creativecommons.org/licenses/by/3.0/de/deed.en
Copyright remains with the author(s).

Citation: Weigl, L. (2026). Strategic compliance narratives: Platform governance under the DMA and DSA. *Internet Policy Review*, *15*(4). https://doi.org/10.14763/2026.4.2129

Keywords: Platform governance, Legal compliance, Digital Services Act, Digital Markets Act

Abstract: Online platform compliance with digital regulation is often framed as a question of effectiveness: whether rules are sufficiently or insufficiently implemented. This paper argues that such a perspective is insufficient for understanding contemporary platform governance. It introduces a new understanding of compliance and develops the concept of 'strategic compliance narratives'. The goal is to capture how designated platforms adapt different regulatory requirements in ways that merely satisfy formal obligations, while also influencing user experience, regulatory legitimacy, and public trust. Based on the theory of legal endogeneity and examples from large online platforms' responses to EU platform regulation it identifies three types of strategic compliance narratives: performative compliance, malicious compliance, and ideological defiance. In doing so, it shifts the focus from whether platforms comply, to how compliance can be enacted. It concludes by outlining policy recommendations to address these strategic dimensions of legal compliance.

Introduction

With a market capitalisation exceeding USD 3 trillion in 2023, Apple is widely regarded as one of the most valuable companies in the world (European Commission, 2024a). As a dominant platform, it navigates a closed ecosystem consisting of hardware, software and digital services. In this position, Apple created its own market rules and imposed restrictions on other market players, including so-called anti-steering practices that restrict developers from informing users about alternative purchasing options outside the App Store. The EU's Digital Markets Act (DMA) was designed to address exactly these kinds of dominant anti-competitive practices. As a response to the DMA, Apple has made a number of changes in the EU since: It allowed third-party app stores and enabled alternative payment options (Apple, 2024); it relaxed the requirement that all browsers have to rely on Apple's own WebKit engine (Ribera Martinez, 2024); and it opened access to the Near Field Communication (NFC) chip used for contactless payments, which for a long time was restricted to Apple's own Apple Pay system, to third-party payment providers (Apple, 2024).

However, Apple's implementation of the DMA also introduced new technical conditions, new review procedures, notarisation procedures, fees, and access requirements that, in practice, continued to position the company as the central gatekeeper of the ecosystem. These changes were met with strong criticism from developers (Roth, 2024a; 2024b), and in April 2025 the European Commission formally found Apple in breach of the DMA's anti-steering obligation and imposed a €500 million fine (European Commission, 2025a). The Commission also issued preliminary findings concerning Apple's terms for alternative app distribution, further indicating that Apple's implementation of the DMA did not fully satisfy the obligations imposed by the regulation (European Commission, 2025b). Yet, while Apple made some DMA-motivated changes and faced regulatory findings of non-compliance, many of the underlying power asymmetries and dependencies within the ecosystem remained.

Parallels can be drawn to some designated tech companies regulated by the Digital Services Act (DSA), which focuses on platform governance, and the risks platforms pose to users and society. Meta, another contentious designated gatekeeper under the DMA, and one of the world's largest digital platforms owning Facebook, WhatsApp, Messenger, Threads, and Instagram, operates recommender systems that determine what billions of users see online day to day. The DSA requires platforms to provide at least one recommender system option not based on profiling, to allow users to freely modify recommendation preferences, and to avoid decep-

tive interface design. Formally, Meta implemented a range of measures intended to comply with the DSA.

In practice, however, the implemented changes did not allow users to directly influence which categories of content are prioritised by the recommendation system itself (Fabbri & Boratto, 2025). The default user experience continued to follow Meta's profiling-based systems (Ašmane & McNamee, 2025). The platform continued with "deceptive" and "unwilled attention-capturing" patterns (Mohanla, 2025). It incorporated the legal requirements in a way that complied with the letter of the law, but left its user engagement-driven model and harmful data practices intact.

These examples introduce the central puzzle of this paper. While online platform compliance with digital regulation is often framed as a question of whether rules are sufficiently or insufficiently implemented, these cases highlight that practice looks much more nuanced. This paper argues that compliance itself can function as a mode of governance through which platforms use the law to serve institutional interests and shape the public perception and discourse. Building on Waldman's (2020) work on legal endogeneity, the paper shows that compliance should not be understood solely as the implementation of legal obligations, but also as a site of contestation where platforms influence how regulation is experienced, evaluated, and legitimised by different audiences. To capture this phenomenon, I develop the concept of *strategic compliance narratives*, defined as the strategic adaptation of regulatory requirements in ways that appear to align with legal frameworks while simultaneously influencing public trust and perceptions of legitimacy.

The concept of strategic compliance narratives is illustrated with examples drawn from the implementation of the DMA and the DSA. Based on platforms' responses to EU platform regulation, it identifies three types of strategic compliance narratives: performative and malicious compliance, concepts already known in policy research, as well as a third type, the one of ideological defiance.

The endogenous dynamics of compliance

Parker and Nielsen (2009) refer to "regulatory capitalism" to describe a social, political, and economic order characterised by the proliferation of markets, as well as state and non-state attempts to regulate. While regulatory capitalism can be understood as an opportunity to use the power of markets to achieve social goods in efficient, effective, and democratically legitimate ways, there is also a critique warning about regulation creating a "smokescreen for ever more self-aggrandising corporate power" (p. 46). Importantly, the "responsibilization of business" and the

"decentering of regulation away from the state" make compliance increasingly difficult to conceptualise. Different regulators, regulated entities, and stakeholders may hold different understandings of what compliance means. Where socially accepted meanings of compliance emerge, they are constructed through interaction among these actors (Parker & Nielsen, 2009; Edelman & Talesh, 2011). To illustrate these dynamics, this article builds on Waldman's (2020) argument about privacy law and legal endogeneity. Waldman contends that compliance mechanisms, such as audits and paper trails, may create an appearance of legal compliance as a symbolic adherence rather than substantive legal protection.

Waldman develops this argument in response to a paradox of today's privacy law. Despite the proliferation of privacy regulation, and despite increasing regulatory attention to data protection, privacy harms continue to persist. He argues that this is because privacy obligations become translated into "managerial" procedures, audits, trainings, assessments, automation of legal decisions, and documentation practices that demonstrate compliance without necessarily advancing the underlying goals of the law: "mere symbols of compliance are standing in for real privacy protections" (ibid., p. 776).

His observation is rooted in Lauren Edelman's theory of legal endogeneity, which suggests that law often becomes shaped by the social fields it seeks to regulate, and was developed by Edelman in the context of Title VII and workplace sex discrimination law (Edelman, 2016). Edelman wanted to understand why, despite the passing of anti-discrimination laws, workplace inequality and discrimination persisted. She found an explanation to this in a concept she termed "legal endogeneity", which describes a process through which the meaning of law is shaped by the organisations it seeks to regulate rather than exclusively by legislators, regulators, or courts. In the case of workplace sex discrimination, rather than enforcing the substantive goals of civil rights law, courts and the Equal Employment Opportunity Commission relied on internal organisational structures, which organisations implemented following the adoption of the Civil Rights Act.

According to Edelman (2016), legal endogeneity runs through a series of six stages (ambiguity/process-oriented law, professional framing, symbolic structures, managerialisation, mobilisation, legal deference, and legal consciousness). Drawing on her account, Waldman describes legal endogeneity as a process through which first, laws are often *ambiguous* and *process-oriented*, giving corporate actors considerable discretion in determining how legal requirements should be operationalised (Waldman, 2020; Nourse & Schacter, 2002; Grundfest & Pritchard, 2002).[1]Second, professional framing. Compliance professionals use the process-

oriented parts of the law and frame its obligations in ways that make them compatible with their companies' own goals. Third, legal requirements become *managerialized*, meaning that compliance is increasingly implemented through internal procedures, reporting systems, audits, and governance structures. Drawing on Cohen (2019), Waldman argues that managerialisation can be understood as an "outgrowth" of a broader neoliberal project that steers regulatory intervention aimed at social welfare objectives towards parameters of efficiency, innovation, and economic growth. Legal obligations become translated into organisational processes designed to facilitate production while minimising regulatory burdens (Blalock, 2015; Cohen, 2019). Fourth, these practices then become *mobilised* as evidence of compliance when organisations are challenged, when they need to defend themselves as employees, citizens, users, data subjects or any other individuals try to vindicate their rights. This essentially discourages rightsholders from taking any legal action in response to rights violations in the first place, and it reconstructs the actual proceeding into a technocratic debate (Bumiller, 1992). Finally, lawyers, judges, and regulators may begin to *defer to such symbolic structures*, whereby "corporate compliance systems become embedded in institutional interpretations of law" (Waldman, 2020, p. 791). Based on Edelman (2016), Waldman describes this final stage of legal endogeneity as developing through three progressive steps: "reference, relevance, and deference." Judges may first mention corporate compliance structures, then treat them as relevant evidence of compliance, and ultimately regard their mere presence as sufficient evidence of lawful conduct (Waldman, 2020, pp. 791-792). As these structures become increasingly associated with legal compliance, they enter collective *legal consciousness*, such that symbolic compliance risks becoming conflated with substantive adherence to the law.

Waldman argues that privacy law exhibits each of these characteristics. The broader consequence is that privacy law is becoming detached from its original purpose. Compliance increasingly serves as indicators of legality, leaving substantive ques-

1. To briefly relate this discussion back to the DSA and DMA, the DSA sits within an approach that combines prescriptive rules with more open-ended obligations and co-regulatory mechanisms, including Codes of Conduct (Husovec, 2024). With regard to legal endogeneity, while Codes of Conduct could strengthen enforcement by providing more detailed standards, there is a risk that their development may also create accountability concerns, that is, allowing the Commission to exercise significant influence over the implementation of the Codes while "bypassing legislative, administrative and public oversight" (Griffin, 2024, p. 185). With regard to the DMA, Tzanaki and Nowag (2026) argue that the DMA's institutional architecture is characterised by decentralised actors and flexible procedures that make its enforcement more participatory, which fits the process-oriented and ambiguous nature of legal endogeneity. Moreover, they highlight the DMA's "cooperative" nature of compliance and dialogue between the Commission, gatekeepers, and third parties, which precedes the traditional punitive enforcement-based model of antitrust. Firms increasingly become "cooperation" partners, reflecting the growing professionalisation and managerialisation of compliance in the different stages of legal endogeneity.

tions about whether privacy is actually being protected unaddressed. Legal endogeneity therefore highlights how organisations participate in the social construction of compliance where requirements are translated, negotiated, and reshaped.

Strategic compliance narratives

Waldman and Edelman help us move from a legalistic understanding of regulation toward a social understanding. Importantly, this social understanding is rooted in a political economy paradigm and standard regulatory theory that views regulation and compliance as interactive processes shaped by the behaviour and interests of both regulators and regulated actors. This is reflected particularly in the idea of responsive regulation (Ayres & Braithwaite, 1992). Responsive regulation emerges from an enforcement pyramid, ranging from cooperation and persuasion at the bottom to increasingly severe sanctions at the top. It also recognises a role for self-regulation and the involvement of public interest groups and citizens. The central idea is that regulation is shaped through interaction between these different actors, rather than being imposed by the state in a one-directional process. In their call for "really responsive regulation", Baldwin and Black (2008) emphasise that regulators must account for the "operating and cognitive frameworks" that is, the strategies and adaptive behaviour of regulated entities. This is particularly relevant in the context of large online platforms, which possess substantial organisational, legal, technical, and communicative resources with which to interpret and operationalise regulatory requirements.

This paper builds on this work and points toward a broader conclusion: If compliance is socially constructed, it can be shaped through interactions among companies, regulators, users, civil society organisations, journalists, and can therefore also have an effect on public perceptions. In other words, regulated entities can not only influence the meaning of the law and its implementation, but also use that influence strategically as a political and communicative tool.

But why is that the case? Why would some companies engage in compliance as a strategic activity? Platforms could treat regulation as a purely legal obligation and approach compliance as a largely technical exercise. And in some instances, this is also the case. This paper is not to argue that every (very large) online platform invests in a strategic plan of compliance. However, what we witness is that very often compliance is becoming increasingly visible through public announcements, compliance websites, executive statements, or blog posts. Compliance therefore becomes a site where the interpretation of regulation is constructed and influenced, which, consequentially, gives companies substantial power in the legal sys-

tem. We arrive, then, at a point where compliance ceases to be a neutral process. The question is therefore no longer simply *whether* platforms comply with regulation, but how compliance is enacted and what its effects are. This paper conceptualises this phenomenon as *strategic compliance narratives*: the strategic adaptation of regulatory requirements in ways that formally align with the legal frameworks while simultaneously influencing public trust and perceptions of legitimacy.

It is important to distinguish the idea of strategic compliance narratives from non-compliance, and regulatory capture or arbitrage. For cases of non-compliance, legal obligations must be clearly violated. According to the logic of strategic compliance narratives, a legal obligation can be formally satisfied, but done in a strategic way to preserve the companies' interests and maintain its market dominance, business model, user engagement, data practices, etc. This also distinguishes strategic compliance narratives from the classic account of regulatory capture. Stigler's (1971) influential theory of economic regulation conceptualises regulation as a potential object of competition among interest groups, with regulated industries seeking to influence regulation in ways that serve their interests. Again, the concept of strategic compliance narratives differs in that, rather than seeking to influence regulators, regulatory agencies or the law itself, regulated entities seek to position themselves toward regulation by shaping the interpretation, implementation, and public understanding of legal requirements. Likewise, the concept is distinct from regulatory arbitrage, in which regulated actors exploit differences or gaps (Marjosola, 2021). Strategic compliance narratives may involve such forms of regulatory arbitrage, but it focuses specifically on how compliance is enacted and communicated: What does compliance look like, how is it understood, and how is it perceived by relevant audiences?

To specify how strategic compliance narratives can be observed in reality, I analysed how Very Large Online Platforms (VLOPs), Very Large Online Search Engines (VLOSEs), and gatekeepers responded to the DSA and to the DMA. In reviewing compliance reports, communications, transparency documentation, platform design changes, policy research, and media coverage of a sample of VLOPs, VLOSEs and gatekeepers, it became apparent that, on the one hand, there is a pattern of legal endogeneity in some way, but also variation in how platforms complied, as well as how they publicly enacted compliance.

Three dimensions proved particularly useful for understanding these variations. I developed them inductively from the reviewed documents and texts, by identifying recurring patterns in how platforms publicly communicate and position themselves, and of course how they substantively implement their obligations. The first

dimension is, thus, *visibility*: how compliance is publicly communicated. Compliance may remain internal and technical, or it may be actively announced on platforms' websites, transparency reports, press releases, executive statements, blog posts, public campaigns, and user-facing design changes. The second dimension is *discursive positioning*. This refers to how platforms frame regulation and their own compliance efforts. Companies may portray regulation as beneficial and cooperative, as burdensome and costly, adopt a more neutral or a heavily political position. The discursive positioning therefore focuses on the construction of narratives about regulation itself. The third dimension is *implementation* and refers to the extent to which regulatory requirements are substantively translated (or not) in practice. This can range from highly procedural or symbolic forms of compliance that satisfy legal requirements, to meaningful and effective implementation of legal obligations.

With these three dimensions we can go into more nuance regarding platforms' compliance strategies. Different combinations of these dimensions reveal different types of strategic compliance narratives. Based on platforms' responses to the DMA and DSA, which will be elaborated on in the next Section of this paper, I identify three such types: performative compliance, malicious compliance, and ideological defiance.

The first two subtypes are not new. Both have appeared in previous scholarship in diverse fields such as sociology and healthcare to describe diverging forms of compliance (Alter, 2015; Greener, 2020; McCarthy et al., 2025). The concept of performative compliance has also appeared in emerging scholarship on platform governance and the DSA. Papaevangelou and Votta (2025) warn that online platforms may strategically use the DSA Transparency Database as a means for "performative compliance" whereby platforms may "strategize their use of the database as a means to show their compliance" (Kaushal et al., 2024, p. 1130). Trans et al. (2024) argue that VLOPs' responses to Article 40 DSA falls under performative compliance, as newly introduced research APIs and data-access mechanisms were presented as evidence of transparency while often providing limited access and unavailable data for the analysis of algorithmic personalisation.

Malicious compliance in the context of EU platform regulation has also appeared in academic research. Studying Apple's response to the DMA, Heimburg et al. (2026) identify malicious compliance as a strategy through which the gatekeeper implemented "changes that reduced functionality or introduced burdensome new terms, with the DMA invoked as a justification for their implementation" (p. 12). Examples include the temporary removal of Progressive Web Apps from the Home

Screen for EU users as a consequence of DMA compliance, which Apple then reversed after public contestation, as well as the introduction of complex contractual arrangements (such as the "Alternative Terms Addendum") that increased administrative burdens and legal complexity for developers (ibid.). Malicious compliance in the context of the DMA was also broadly featured in the news. The digital rights organisation EDRi highlighted how Apple's implementation of DMA requirements formally enabled alternative app stores and browser engines, while making sure to maintain many of the practical barriers that users and app developers face (European Digital Rights, 2024). Politico (Hancock, 2024) described parts of Google's and Apple's DMA implementation as forms of malicious compliance, arguing that platform design changes framed as EU regulatory obligations imposed new frictions on users. Related arguments have been expressed by authors at Tech Policy Press (Dempsey & Stasi, 2025) and by Proton founder Andy Yen (2024), who argue that some DMA obligations allow gatekeepers to maintain their control without realising the benefits for users and developers that the regulation was intended to create. In the context of the DSA, the NGO EU DisinfoLab (Ašmane & McNamee, 2025) identifies malicious compliance based on examples of Meta's recommender systems and transparency obligations.

Building on these existing discussions, I adopt performative compliance and malicious compliance into the broader framework of strategic compliance narratives.

- *Performative compliance* refers to visible and positively framed compliance efforts with limited substantive implementation. The objective is to produce legitimacy (trust in the regulated entity).
- *Malicious compliance* refers to the implementation of a legal obligation in a way that satisfies formalities while undermining its intended purpose. The objective is friction (distrust in the regulation).

I also suggest a third type that has received less attention in compliance literature: ideological defiance. This concept emerged inductively from observations that did not fit neatly within these two existing types. While performative and malicious compliance are characterised by relatively visible compliance and more limited or problematic implementation, there is also discursive positioning that is much more politicised and value-laden (beyond a merely positive or negative framing), and extended beyond individual regulatory requirements themselves. It may come to no surprise that this category was inspired by X as an outlier in this respect, but I nevertheless consider this pattern important because the involvement of powerful political and business figures means that such compliance narratives can have effects far beyond platform governance itself.

- *Ideological defiance* refers to a confrontational form of compliance in which regulated entities frame regulation as illegitimate or politically objectionable while implementing requirements to a limited or to no extent at all. The objective is opposition (distrust in the regulator).

The following section illustrates each type through platform responses to the DMA and DSA.

Illustrative cases of strategic compliance narratives

Performative compliance

As a designated very large online platform, TikTok is a perfect illustration of performative compliance. Shortly after the DSA entering into force, it published a dedicated website in August 2023 for the new EU regulation announcing its compliance efforts (Moncrieff, 2023). It also has a dedicated "transparency" site through which to access regional compliance information. Among this information, TikTok publishes detailed DSA compliance reporting information, including the yearly transparency reports, as well as risk assessments and audit reports linked to Articles 34 and 35 DSA (TikTok, 2026a).

In announcing its DSA compliance in August 2023, TikTok stated that "with this scale comes significant responsibility" and described compliance with the regulation as a responsibility it was "embracing." More than 1,000 employees were reportedly involved in preparing for the DSA, and TikTok repeatedly presents the regulation as an opportunity to increase transparency, user choice, and online safety. The platform even describes the DSA as a "landmark piece of content safety legislation". TikTok also announced the launch of its European Online Safety Hub specifically designed to explain its compliance activities to users, ranging from content moderation to recommender systems, research, transparency and teen safety. Once again, on the hub's website, TikTok argued that "[it] embrace[s] regulatory transparency and accountability requirements such as those set out in the Digital Services Act" (TikTok, 2026b).

With regard to more detailed obligations set out in the DSA, TikTok highlights compliance efforts specifically related to

- new reporting options for illegal content (Art. 16, 17 and 20 DSA),
- non-personalised recommendation options (Art. 38 DSA),
- a repository providing information on paid advertisements (Art. 39 DSA),
- researcher API access, (Art. 40 DSA),
- advertising labelling tools (Art. 26 DSA),

- and restrictions on personalised advertising for minors (Art. 28 DSA)

This showcasing of compliance measures can be found repeatedly in TikTok's *Newsroom*. To name another example, in October 2024, after publishing their third transparency report on content moderation, TikTok proudly highlighted that it removed more than 22 million pieces of content, that they banned more than 5 million accounts, and received around 144.000 illegal content reports of which almost 30% were found to violate their policies or local law. While such figures create an impressive appearance of transparency and accountability, Keller (2024) made a point by arguing that metrics like those above primarily make compliance measurable, rather than trustworthy. Numbers reveal information about content moderation activity, but remain difficult to benchmark and even more difficult to use to assess whether content moderation is successful.

In terms of our three dimensions (visibility, discursive positioning and implementation), we can see that TikTok's compliance efforts were very visibly demonstrated and combined with a strongly cooperative and positive discursive positioning. Implementation went a different path. Article 27 of the DSA, for instance, requires providers to explain "in their terms and conditions, in plain and intelligible language, the main parameters used in their recommender systems […] as well as any options for the recipients of the service to modify or influence those main parameters". TikTok is giving a high-level overview of those parameters. It also allows users to control the parameters by adding filters for specific words or hashtags from the content preferences section in the user settings, while also recommending users to unfollow accounts in order to remove their posts from users' feed (TikTok, 2026c). Keyword filtering may reduce exposure to specific topics, but it requires specific anticipation, awareness and knowledge of content a user may want to hide, and does not give users meaningful influence over the underlying recommendation logic that determines what content is amplified or suppressed. Moreover, according to Article 38, users can opt to have a non-personalised feed. While TikTok does provide such an alternative feed, it does not give users meaningful agency over content curation. Hence, the usefulness of TikTok's implementation of this option is "quite debatable" and can be described as a form of "transparency washing" (Reviglio & Fabbri, 2024).

A further example concerns TikTok's management of systemic risks under Articles 34 and 35 DSA. While TikTok repeatedly emphasised its commitment to election integrity and risk mitigation, the Romanian presidential election became a major controversy. In December 2024, Romania's Constitutional Court annulled the results of the first round of the presidential election following findings that Russian

influence operations had manipulated social media to promote the independent nationalist candidate Călin Georgescu. This case clearly exposed failures in TikTok's implementation of the DSA's risk-management obligations. Radu (2025) argues that TikTok failed to provide meaningful transparency regarding political content and electoral risks. Similarly, Albert (2024) notes that concerns were raised regarding TikTok's handling of political content, paid influencers, and recommender-system risks, as well as implemented risk mitigation measures in the Romanian context.

These are just a few examples of a recurring pattern: TikTok's DSA compliance was made highly visible and framed in strongly cooperative terms, while the effectiveness of several implementation measures remained very weak: For example, regarding the risk-management obligations under Articles 34 and 35, the Commission opened multiple formal proceedings against TikTok in 2024 concerning, among other things, the risk management of addictive design and harmful content (European Commission, 2024b), the risk assessment and mitigation measures associated with TikTok Lite (European Commission, 2024c), and systemic risks to election integrity (European Commission, 2024d). In February 2026, the Commission preliminarily found TikTok in breach of the DSA in relation to its addictive design (European Commission, 2026a). With regard to Article 39, the Commission opened formal proceedings in February 2024 and preliminarily found TikTok in breach of the DSA in May 2025 because its advertisement repository did not provide the necessary information about advertisements, while also limiting comprehensive public searches of this information (European Commission, 2025c). In October 2025, the Commission also preliminarily found TikTok in breach of its obligation under Article 40 to provide researchers with adequate access to public data (European Commission, 2025d). And in July 2026 TikTok was preliminarily found to breach Article 28 for failing to ensure safe and accounts for minors (European Commission, 2026b).

The case therefore illustrates what this paper conceptualises as performative compliance: a form of compliance in which visibility of compliance efforts and positive framing of the regulation itself are supposed to generate legitimacy and trust, despite a lack of meaningful and substantive realisation of the regulatory objectives.

Malicious compliance

A very good illustration for malicious compliance is Apple's compliance with the DMA. Prior to the DMA, Apple required developers to use its in-app payment system, restricted anti-steering practices, limited sideloading, and charged commis-

sions of up to 30% on many transactions (European Commission, 2020). On iOS, Apple required all browsers to use its own WebKit engine, turning Chrome, Firefox, and others into variations of Safari (Lomas, 2024). And for a long time, access to certain hardware features like the Near Field Communication (NFC) chip used for contactless payments was reserved for Apple's own Apple Pay system, reinforcing how much leverage Apple has to favour its own solution (Loser, 2024).

Following its designation as a gatekeeper, Apple created a dedicated DMA information page through which one can access its latest version of its DMA compliance report (Apple, 2026a). Further, in its Apple Developer site, Apple curates a long page of updates on apps distributed in the EU, which enlists detailed explanations of the changes implemented in the EU. This includes support for alternative app marketplaces (Art. 6(4) DMA), alternative payment options and anti-steering provisions (Art. 5(4), 5(7) DMA), third-party browser engines (Art. 5(7), 6(4) DMA), and NFC interoperability for payment services (Art. 6(7) DMA) (Apple, 2026b).

However, unlike TikTok's cooperative framing of EU legislation, Apple's discursive positioning towards the DMA goes into a more defensive and sometimes even accusing direction. Apple repeatedly frames the DMA as a source of security, privacy, and user-experience risks, as shown by the following excerpts:

> *"We strive to earn users' trust by promptly resolving issues with apps, purchases, or web browsing through App Review, AppleCare customer support, and more. The DMA requires changes to this system that bring greater risks to users and developers. This includes new avenues for malware, fraud and scams, illicit and harmful content, and other privacy and security threats."* (Ibid.)

> *"Instead of one trusted place to get apps, EU users now face multiple marketplaces, each with their own design, rules, and review standards. On other mobile platforms, that leads to harmful look-alike apps that slip through with fewer checks, and marketplaces where users don't know where to turn if something goes wrong. Apple users in the EU are now more likely to face those same risks."* (Ibid.)

Implementation also reveals a pattern consistent with malicious compliance. Although Apple implemented several DMA-motivated changes, it did so in a way that would still maintain a closed ecosystem and allow for self-preferencing in a different way. Third-party app stores remained subject to notarisation and new complex

fee structures, such as Apple's contentious Core Technology Fee. In April 2025, the Commission preliminarily found that Apple's conditions for alternative app distribution did not comply with Article 6(4), arguing that the Core Technology Fee and other requirements discouraged developers from using alternative distribution channels and that the installation of apps through these channels was overly burdensome for users (European Commission, 2025b). Alternative browser engines also required authorisation and were restricted to EU-only versions, forcing alternative browsers to maintain separate app infrastructures and creating additional costs and barriers; and access to NFC functionality continued to operate through newly introduced interoperability conditions (Lomas, 2024; Ribera Martinez, 2024). The Commission's enforcement action also addressed Apple's anti-steering practices. In April 2025, it found Apple in breach of Article 5(4) and imposed a €500 million fine, concluding that Apple's restrictions prevented developers from fully informing users about cheaper alternatives and steering users to offers outside the App Store (European Commission, 2025a). Apple also justified the delayed launch of its AirPods Live Translation feature in the EU based on the DMA's interoperability requirements, which it argued to create additional privacy and security challenges. The decision to provisionally exclude European users from this feature left EU regulators unable "to understand the nature of Apple's ecosystem" who reiterated that the "DMA does not impede the launch of new products in EU markets. To the opposite, it preserves innovation and freedom of choice" (Haeck & Parry, 2025). In fact, it can be questioned whether the delay was technically necessary, arguing that interoperability was framed as a privacy risk, while Apple allows comparable live-translation services across non-proprietary devices. As one critic noted: "why does Apple even let banking apps, medical apps, or location-based software like map apps into the App Store?" (Sorrel, 2026). This suggests that the restricted AirPods function served less to protect user privacy than to portray the regulation itself as harmful to users.

In terms of the three dimensions identified in this paper, Apple's DMA compliance combined high visibility with a largely defensive discursive positioning and a disappointing implementation of legal obligations. Malicious compliance created friction and questioned the legitimacy of the regulatory intervention itself.

Ideological defiance

Compared to TikTok and Apple, X placed far less emphasis on making its compliance activities visible. While the platform maintains a Transparency Center and publishes the legally mandated reports (transparency, risk assessment, audit, and audit implementation reports), as well as information on moderation and enforce-

ment statistics, references to the DSA are limited (X Corp., 2026). Rather than mentioning DSA compliance initiatives, X frames its transparency and online safety efforts through its own platform rules, emphasising their own "X rules" in order to "disrupt global state-backed information operations."

X's discursive positioning towards the DSA has been markedly more confrontational. X and owner Elon Musk have repeatedly framed the DSA as a threat to free expression (Jahangir, 2025). Similar narratives have been voiced by Musk's political allies, who view the DSA as an attempt to regulate public discourse. (DiResta & Jackson, 2025) The chairman of the US Federal Communications Commission, for instance, claimed the DSA to be "incompatible with America's free speech tradition" (Mukherjee, 2025).

Scholars have argued that the transformation of Twitter into X under Musk was accompanied by a shift towards "platform illiberalism," characterised by ambiguous 'illiberal-esque' logics to govern content on the platform, and the mobilisation of this logic to support illiberal actors operating beyond the platform (Magalhães et al., 2026). In fact, this 'backsliding' has materialised in a hard libertarian platform ideology based on an odd understanding of "free speech", with Musk describing himself as a "free speech absolutist" (ibid, p. 10). The acquisition of X by Musk was followed by extensive cuts in X's content moderation teams, dismantling Trust & Safety departments, amplifying right-wing content, and reversing previous account suspensions and bans (van de Kerkhof, 2025; Warzel, 2023).

With regard to DSA implementation, a first strong sign of X's and Musk's resistance was the withdrawal from the voluntary Code of Practice on Disinformation in May 2023, which, established in 2018, became a recognised Code of Conduct under the DSA later on. An analysis of platforms' self-assessment of the code revealed that "the inescapable conclusion of this document is that Elon Musk's Twitter failed every single indicator and gave every impression of blatant non-compliance (e.g., by selfplagiarising much of their report from previously published boilerplate text)" (Park et al., 2023, p. 12).

It is important to preface these implementation failures have not gone unnoticed. In 2025, the European Commission imposed a fine on X of €120 million for breaches of several DSA obligations, including the deceptive design of its verification system ('blue checkmarks') under Article 25(1), the lack of transparency in its advertising repository under Article 39, and failures to provide researchers with access to public data under Article 40(12) (European Commission, 2025e). In January 2026, the Commission also opened formal proceedings under Articles 34 and 35 to in-

vestigate whether X had adequately assessed and mitigated systemic risks associated with the deployment of Grok and its recommender systems (European Commission, 2026c). But besides that, X's implementation performance of many of the remaining DSA obligations has been unsurprisingly meagre. Article 37 DSA mandates that the designated VLOPs and VLOSEs undergo annual, independent audits to assess compliance with risk assessment and mitigation (Art. 34, Art. 35). Just like X's risk assessment report – which is extensively redacted compared to those of other platforms making meaningful public scrutiny nearly impossible – its first DSA audit also differed from those of other designated platforms. Whereas most auditors issued positive opinions, positive with comments, or disclaimers of opinion, X's auditor, FTI Consulting, issued several negative findings regarding the platform's compliance. The auditor identified gaps in X's assessment and mitigation of systemic risks associated with recommender systems, content moderation, advertising practices, and data use (FTI Consulting, 2024). The audit outcome per se is unsurprising. X's response is much more interesting: Rather than implementing the auditor's recommendations, X largely dismissed the findings (Albert, 2025). Even more, in the following audit cycle the year after, X replaced FTI Consulting with a new auditor, BDO (ibid.). In doing so, X essentially weakened one of the few mechanisms of independent oversight within the DSA audit framework, thereby not only dismissing the first negative findings it received, but also signalling its unwillingness to subject itself to the DSA's systemic risk assessment and mitigation regime.

In terms of the three dimensions identified in this paper, X combined comparatively low compliance visibility with a very confrontational discursive positioning and a limited – I'd dare to say even provocative – implementation of DSA obligations. Unlike malicious compliance, which seeks to scapegoat and 'burden-frame' regulation while formally adhering to it, X's approach was an ideological contestation of regulatory authority itself. The objective was to portray the DSA and EU regulators as political threats to free expression. X's strategy exemplifies what I conceptualise as ideological defiance.

Consequences for platform governance

Legal endogeneity in platform regulation

The cases examined in this article support the central argument of legal endogeneity theory. Both the DSA and the DMA contain a range of open-ended and process-oriented obligations whose practical meaning is not self-evident. Concepts such as interoperability, user choice, systemic risk, risk mitigation, transparency, and accountability require substantial interpretation and operationalisa-

tion by regulated platforms. This ambiguity creates room for corporate actors to shape how compliance is understood and implemented. As Edelman (2016) and Waldman (2020) argue, legal uncertainty enables compliance professionals to translate legal obligations into their own organisational practices that remain compatible with existing business models.

The implementation of both regulations demonstrates precisely this dynamic. Many obligations are fulfilled through managerial processes such as risk assessments, transparency reports, audits, compliance reports, and internal procedures (Griffin, 2025; Martínez, 2025). Compliance therefore becomes increasingly expressed through documentation, quantification, and reporting. Particularly under the DSA, highly complex social phenomena such as disinformation, electoral integrity, fundamental rights risks, or recommender-system harms are translated into risk-management procedures, indicators, and audit processes. Similarly, under the DMA, obligations intended to increase contestability and reduce gatekeeper power are operationalised through technical compliance mechanisms, and transformed into counterproductive rules, such as notarisation procedures or new fee structures.

The cases highlight how these organisational structures are subsequently mobilised as evidence of compliance. Documentation and box-ticking exercises become the primary objects through which regulators, auditors, and the public evaluate platform behaviour. The question shifts from whether societal risks have actually been reduced or market power has actually been constrained to whether the required procedures, reports, and compliance mechanisms have been submitted or implemented on time. In this sense, the DSA and DMA increasingly demonstrate features of the symbolic structures identified by legal endogeneity theory.

Strategic compliance narratives as a political and communicative practice

The cases presented in this paper suggest an argument in which compliance serves a strategic function: a political and communicative practice through which platforms actively shape public perceptions of legitimacy and trustworthiness of platforms, regulation and regulatory authority. Transparency reports, risk assessments, compliance reports, audit documents, and public statements do not only serve managerial or mobilising functions. They can create narratives about the platform and the regulation, which in turn impacts the perceptions of a range of actors in the network: users, media, citizens, policy-makers, etc.

TikTok framed compliance as a demonstration of responsibility and credibility. Apple portrayed the DMA as creating privacy, security, and innovation risks, thereby creating friction and distrust in the regulation. And X challenged the legitimacy of the regulatory authority itself. In doing so, the platform positioned itself to align closely with the Trump administration and other US political actors, who portrayed the DSA as a European censorship tool.

The concept of strategic compliance narratives therefore shifts attention away from compliance as a regulatory outcome and towards compliance as strategy to shape public legitimacy and trustworthiness. The importance of this dynamic needs to be emphasized, as the consequences for user and citizen perceptions can be misplaced trust and distrust in platforms and institutions respectively. If not addressed, this can affect the perceived legitimacy of regulation and increase corporate power over regulatory meaning.

Implications for platform governance and compliance

Beyond procedure. To counter the consequences outlined above, platform governance should move beyond process-oriented, check-box compliance, which, of course, is difficult to implement. Through performative compliance, TikTok demonstrates how extensive reporting and transparency can create an image of responsibility without necessarily proving substantive effectiveness. Through malicious compliance, Apple shows how legal obligations can be implemented formally while preserving the underlying business model. And through ideological defiance, X demonstrates how audit and risk-management mechanisms can be engaged in ways that undermine their intended purpose. The mere existence of compliance artefacts should therefore not be treated as evidence of successful regulatory outcomes. Baldwin and Black (2008) argue that the assessment of compliance requires regulators to develop meaningful benchmarks against which the effectiveness of compliance measures can be assessed, rather than relying solely on procedural indicators. However, such benchmarks are not necessarily immune from strategic behaviour. As the cases discussed in this paper illustrate, regulated entities may adapt their practices to the criteria used to assess compliance, potentially turning these indicators into new forms of procedural compliance. It is rather recommended that regulators refrain from over-outsourcing oversight functions to third-party corporations, and design regulatory obligations ex ante in ways that limit the extent to which companies can rely on procedures as substitutes for substantive compliance. This also requires greater involvement of the groups that regulation is intended to protect or empower. Consumer protection organisations, user advocacy groups, SME, developer, and industry associations should be given direct

opportunities and most importantly resources to provide evidence on the practical effects of platform compliance (Cseres & de Korte, 2025). Another way of counterbalancing this "proceduralism" is to strengthen private and collective enforcement mechanisms. Collective actions can enable consumers, SMEs, and other business users to overcome the practical barriers that often prevent individual enforcement against powerful gatekeepers (Hornkohl & Ribera Martínez, 2024). Strengthening such mechanisms would introduce additional actors into the enforcement process and provide those affected by platform practices with a means of challenging the interpretation and implementation of regulatory obligations independently of the regulator-platform relationship.

Legal guidance. Many of the DSA and DMA's central concepts – systemic risks, risk mitigation, interoperability, fairness – are subject to ambiguity and require substantial interpretation. Apple's DMA implementation in particular illustrates how platforms may formally comply with legal requirements while interpreting them in ways that preserve existing business models and limit the practical effects of regulation. To reduce opportunities for corporate interpretation and managerializsation, regulators should intervene early in the interpretive process. Regulators need to provide detailed guidance on the interpretation obligations through implementing acts and guidelines. As Waldman notes, rulemaking can help clarify statutory requirements, provide greater legal certainty, and prevent regulated entities from becoming the primary interpreters of their own obligations.

Independent oversight. A third implication concerns compliance reporting and third-party oversight through audits. The X case illustrates how compliance mechanisms intended to provide independent scrutiny can themselves become vulnerable to strategic manipulation. X's decision to replace its initial auditor following critical findings raises concerns about auditor shopping and the risk of audit capture. These developments question whether current audit regimes provide sufficiently independent and useful oversight of platform compliance. Rather than relying exclusively on private audit firms, future oversight mechanisms should incorporate a broader range of actors, including academic researchers, civil society organisations, and other independent experts (Weigl et al. 2026).

Conclusion

This paper examined how large digital platforms publicly responded to the EU's DSA and DMA. It argued that legal compliance is not merely an outcome but a communicative and political process. Building on the literature on legal endogeneity, the paper showed how the ambiguity and process-oriented nature of platform

regulation creates space for platforms to shape the meaning of compliance.

To capture this phenomenon, the paper introduced the concept of *strategic compliance narratives*, defined as the strategic adaptation of regulatory requirements in ways that formally align with legal obligations while simultaneously influencing public trust and perceptions of legitimacy. Through the cases of TikTok, Apple, and X, three types of compliance narratives were identified: *performative compliance*, which seeks to generate trust in the regulated entity; *malicious compliance*, which creates friction and distrust toward the regulation itself; and *ideological defiance*, which challenges the legitimacy of the regulatory authority. The findings suggest that compliance can function as a tool for legitimacy-building, political positioning, and regulatory contestation.

The paper also offers recommendations for regulatory design and enforcement. Regulators should move beyond procedural indicators of compliance, strengthen the involvement of affected stakeholders and independent actors in assessing substantive outcomes, and provide clearer guidance where regulatory obligations leave substantial room for corporate interpretation.

This study has several limitations. Most importantly, the analysis relied on three illustrative case studies, raising questions about generalisability. Future research should examine whether similar patterns emerge across a broader range of platforms. Preliminary observations suggest that the identified narratives may also include Google showing forms of malicious compliance under the DMA and Meta engaging in a more performative compliance strategy under the DSA. YouTube's transparency reporting under the DSA also provides a potentially relevant case for examining performative compliance.

Future work could also explore why certain regulatory frameworks appear to trigger different compliance narratives: Performative compliance appears to be related to the DSA, while malicious compliance appears to be a strategy adopted under the DMA. One assumption could be that under the DSA, obligations relate to transparency, online safety, and risk mitigation, and can serve as ideal public announcements and evidence of corporate responsibility. By contrast, the DMA directly targets business practices and platforms' market power and compliance also often entails material economic costs. Under such conditions, firms may have stronger incentives to engage in forms of malicious compliance to preserve existing business. Therefore, the nature of the regulatory obligation itself may shape the type of compliance narrative that emerges, but whether this theory extends beyond the cases examined here remains an open empirical question.

References

Albert, J. (2024, December 20). *TikTok and the Romanian elections: A stress test for DSA enforcement - DSA Observatory*. https://dsa-observatory.eu/2024/12/20/tiktok-and-the-romanian-elections/

Albert, J. (2025). What are DSA audits doing for systemic risk enforcement? The case of X. *DSA Observatory*. https://dsa-observatory.eu/2025/12/19/dsa-audits-what-are-they-good-for/

Alter, S. (2015). Beneficial noncompliance and detrimental compliance: Expected paths to unintended consequences. *AMCIS 2015 Proceedings*. https://aisel.aisnet.org/amcis2015/AdoptionofIT/GeneralPresentations/19

Apple. (2024, January 25). Apple announces changes to iOS, Safari, and the App Store in the European Union. *Newsroom*. https://www.apple.com/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/

Apple. (2026a). Changes for apps in the European Union. *Apple Developer*. https://developer.apple.com/support/apps-in-the-eu

Apple. (2026b). European Digital Markets Act (DMA). *Apple Legal*. https://www.apple.com/legal/dma/

Ašmane, K. L., & McNamee, J. (2025). Malicious semi-compliance as platform approach to EU regulation. *EU DisinfoLab*. https://www.disinfo.eu/malicious-semi-compliance-as-platform-approach-to-eu-regulation/

Ayres, I., & Braithwaite, J. (1995). *Responsive regulation: Transcending the deregulation debate*. Oxford University Press.

Baldwin, R., & Black, J. (2008). Really responsive regulation. *The Modern Law Review*, *71*(1), 59–94. https://doi.org/10.1111/j.1468-2230.2008.00681.x

Belloso, N. M. (2024, April 3). A DMA compliance saga: Europe and progressive web apps. *CEPA*. https://cepa.org/article/a-dma-compliance-saga-europe-and-progressive-web-apps/

Blalock, C. (2015). Neoliberalism and the crisis of legal theory. *Law and Contemporary Problems*, *77*(4), 71–103.

Bumiller, K. (1992). *The civil rights society*. Johns Hopkins University Press. https://doi.org/10.56021/9780801835445

Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press.

Cseres, K. J., & Korte, L. C. de. (2025). Participation of third parties in the public enforcement of the Digital Markets Act: Between democracy and technocracy. *Journal of Antitrust Enforcement*, *13*(3). https://doi.org/10.1093/jaenfo/jnae051

Deene, J. (2025, October 2). Can Meta just reset your choice of chronological feed? *ICT Lawyer*. https://www.ictrechtswijzer.be/en/can-meta-just-reset-your-choice-of-chronological-feed/

Dempsey, M., & Stasi, M. L. (2025). What Europe's Digital Markets Act has delivered so far and what comes next. *Tech Policy Press*. https://www.techpolicy.press/what-europes-digital-markets-act-has-delivered-so-far-and-what-comes-next/

DiResta, R., & Jackson, D. (2025). Regulation or repression? How the right hijacked the DSA debate. *Lawfare*. https://www.lawfaremedia.org/article/regulation-or-repression--how-the-right-hijacked-the-dsa-debate

Edelman, L. B. (2016). *Working law: Courts, corporations, and symbolic civil rights*. University of Chicago Press. https://press.uchicago.edu/ucp/books/book/chicago/W/bo24550454.html

Edelman, L., & Talesh, S. A. (2011). To comply or not to comply-that isn't the question: How organizations construct the meaning of compliance. *Explaining Compliance: Business Responses to Regulation*, 103–122.

European Commission. (2020, June 16). Antitrust: Commission opens investigations into Apple's App Store rules. *Press Corner*. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1073

European Commission. (2024a). *Commission decision case AT.40437 – Apple – App Store practices (music streaming)*.

European Commission. (2024b, February 19). Commission opens formal proceedings against TikTok under the Digital Services Act. *Press Corner*. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_926

European Commission. (2024c, April 22). Commission opens proceedings against TikTok under the DSA regarding the launch of TikTok Lite in France and Spain, and communicates its intention to suspend the reward programme in the EU. *Press Corner*. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2227

European Commission. (2024d, December 17). Commission opens formal proceedings against TikTok over suspected DSA breaches related to Romanian elections. *Press Corner*. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487

European Commission. (2025a, April 23). *Commission finds Apple and Meta in breach of the Digital Markets Act* [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085

European Commission. (2025b, April 23). Commission preliminarily finds Apple in breach of the Digital Markets Act's rules on alternative app distribution. *Press Corner*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1086

European Commission. (2025c, May 15). Commission preliminarily finds TikTok's ad repository in breach of the Digital Services Act. *Press Corner*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1223

European Commission. (2025d, October 24). Commission preliminarily finds TikTok and Meta in breach of their transparency obligations under the Digital Services Act. *Press Corner*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2503

European Commission. (2025e, December 5). Commission fines X €120 million under the Digital Services Act. *Press Corner*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2934

European Commission. (2026a, January 26). Commission investigates Grok and X's recommender systems under the Digital Services Act. *Press Corner*. https://ec.europa.eu/commission/presscorner/detail/en/ip_26_203

European Commission. (2026b, February 6). Commission preliminarily finds TikTok's addictive design in breach of the Digital Services Act. *Press Corner*. https://ec.europa.eu/commission/presscorner/detail/en/ip_26_312

European Commission. (2026c, July 24). Commission preliminary finds TikTok in breach of Digital Services Act for failing to ensure safe accounts for minors. *Press Corner*. https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1679

European Digital Rights. (2024). *How tech corporations subvert the EU's new digital laws*. https://edri.org/our-work/delay-depress-destroy-how-tech-corporations-subvert-the-eus-new-digital-laws/

Fabbri, M., & Boratto, L. (2025). Auditing recommender systems for user empowerment in Very Large Online Platforms under the Digital Services Act. *Proceedings of the Nineteenth ACM Conference on Recommender Systems, RecSys '25*, 51–61. https://doi.org/10.1145/3705328.3748074

FTI Consulting. (2024). *X independent audit Article 37 of Regulation (EU) 2022/2065 (Digital Services Act)*. https://transparency.x.com/en/reports/dsa-audit-report

Gomez, C., & Schoch, L. (2026). Safeguarding in sport: Toward a performative compliance of international sports federations? *International Review for the Sociology of Sport*, 10126902251404389. https://doi.org/10.1177/10126902251404389

Greener, J. (2020). Performative compliance and the state–corporate structuring of neglect in a residential care home for older people. *Critical Criminology*, *28*(4), 651–668. https://doi.org/10.1007/s10612-019-09467-3

Griffin, R. (2024). Codes of conduct in the Digital Services Act: Functions, benefits & concerns. *Technology and Regulation*, *2024*, 167–187. https://doi.org/10.71265/a54szq76

Griffin, R. (2025). The politics of risk in the Digital Services Act: A stakeholder mapping and research agenda. *Weizenbaum Journal of the Digital Society*, *5*(2), Article 2. https://doi.org/10.34669/wi.wjds/5.2.6

Grundfest, J. A., & Pritchard, A. C. (2002). Statutes with multiple personality disorders: The value of ambiguity in statutory design and interpretation. *Stanford Law Review*, *54*(4), 627. https://doi.org/10.2307/1229575

Haeck, P., & Parry, J. (2025). Apple blocks translation AirPods in EU over regulatory concerns. *Politico*. https://www.politico.eu/article/apple-blocks-airpods-translation-eu-because-regulation/

Hancock, E. (2024, March 24). *'Severe pain in the butt': EU's digital competition rules make new enemies on the internet*. https://www.politico.eu/article/european-union-digital-markets-act-google-search-malicious-compliance/

Hartzog, W. (2018). *Privacy's blueprint: The battle to control the design of new technologies*. Harvard University Press.

Heimburg, V., Verlooy, V., Staudacher, F., & Schreieck, M. (2026). The gatekeeper's gambit: How platforms strategically adapt to platform regulation. *ECIS 2026 Proceedings*. https://aisel.aisnet.org/ecis2026/is_policy/is_policy/5

Hornkohl, L., & Ribera Martínez, A. (2024). Collective actions and the Digital Markets Act: A bird without wings. *The Antitrust Bulletin*, *70*(1), 3–60. https://doi.org/10.1177/0003603X241296560

Husovec, M. (2024). The DSA as a co-regulatory system. In M. Husovec (Ed.), *Principles of the Digital Services Act* (p. 0). Oxford University Press. https://doi.org/10.1093/law-ocl/9780192882455.003.0020

Jahangir, R. (2025). Understanding the EU's Digital Services Act enforcement against X. *Tech Policy Press*. https://www.techpolicy.press/understanding-the-eus-digital-services-act-enforcement-agains

t-x/

Kaushal, R., Kerkhof, J. van de, Goanta, C., Spanakis, G., & Iamnitchi, A. (2024). *Automated transparency: A legal and empirical analysis of the Digital Services Act transparency database* (arXiv:2404.02894). arXiv. https://doi.org/10.48550/arXiv.2404.02894

Keller, D. (2024). The rise of the compliant speech platform. *Lawfare*. https://www.lawfaremedia.org/article/the-rise-of-the-compliant-speech-platform

Levine, J. (2026, May 5). Introducing the mobile trilemma. *Tech Policy Press*. https://www.techpolicy.press/introducing-the-mobile-trilemma/

Lomas, N. (2024, January 26). A closer look at Apple's browser-related changes to iOS in EU. *TechCrunch*. https://techcrunch.com/2024/01/26/apple-dma-webkit/

Loser, P. (2024, January 30). Apple mobile payments: Evaluating the proposed commitments to the European Commission. *Kluwer Competition Law Blog*.

Magalhães, J. C., Iglesias Keller, C., & Gorwa, R. (2026). The great sysop: Elon Musk, X, and the emergence of platform illiberalism. *New Media & Society*, 14614448261424889. https://doi.org/10.1177/14614448261424889

Marjosola, H. (2021). The problem of regulatory arbitrage: A transaction cost economics perspective. *Regulation & Governance*, *15*(2), 388–407. https://doi.org/10.1111/rego.12287

Martínez, A. R. (2025). The credibility of the DMA's compliance reports. *World Competition*, *48*(1). https://testcdn.kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\WOCO\WOCO2025009.pdf

McCarthy, M., Riddle, S., & Hickey, A. (2025). The teacher as double agent: Performative compliance, allegiance and survival in the contemporary classroom. *Teachers and Teaching*, *31*(8), 1251–1265. https://doi.org/10.1080/13540602.2025.2478150

Mohanla, C. (2025). Investigation: Platforms still use manipulative design despite DSA rules - DSA Observatory. *DSA Observatory*. https://dsa-observatory.eu/2025/08/07/investigation-platforms-still-use-manipulative-design-despite-dsa-rules/

Moncrieff, M. (2023, August 28). Our compliance with the Digital Services Act. *TikTok Newsroom*. https://newsroom.tiktok.com/compliance-digital-services-act-eu?lang=en-150

Mukherjee, S., & Mukherjee, S. (2025, March 3). US FCC chair says EU Digital Services Act is threat to free speech. *Reuters*. https://www.reuters.com/technology/eu-content-law-incompatible-with-us-free-speech-tradition-says-fccs-carr-2025-03-03/

Nourse, V., & Schacter, J. (2002). The politics of legislative drafting: A congressional case study. *NYU Law Review*, *77*(3).

Papaevangelou, C., & Votta, F. (2025). Trading nuance for scale? Platform observability and content governance under the DSA. *Internet Policy Review*, *14*(3), 1–31. https://doi.org/10.14763/2025.3.2037

Park, K., Mündges, S., Brautovic, M., Culloty, E., Holford, D., Kozyreva, A., Lewandowsky, S., Meyer, T., & Wegner, S. (2023). *CoP Monitor: Baseline reports: Assessment of VLOP and VLOSE signatory reports for the strengthened code of practice on disinformation*. Dublin City University Institute of Future Media, Democracy and Society (FuJo).

Parker, C., & Nielsen, V. (2009). The challenge of empirical research on business compliance in regulatory capitalism. *Annual Review of Law and Social Science*, *5*, 45–70. https://doi.org/10.1146/annurev.lawsocsci.093008.131555

Perez, S. (2025, June 26). Apple updates the rules for its EU App Store by adding more complicated fees. *TechCrunch*. https://techcrunch.com/2025/06/26/apple-updates-the-rules-for-its-eu-app-store-by-adding-more-complicated-fees/

Radu, R. (2025). TikTok, Telegram, and trust: Urgent lessons from Romania's election. *TechCrunch*. https://www.techpolicy.press/tiktok-telegram-and-trust-urgent-lessons-from-romanias-election/

Reviglio, U., & Fabbri, M. (2024). The regulation of recommender systems under the DSA: A transition from default to multiple and dynamic controls? - DSA Observatory. *DSA Observatory*. https://dsa-observatory.eu/2024/11/22/the-regulation-of-recommender-systems-under-the-dsa-a-transition-from-default-to-multiple-and-dynamic-controls/

Ribera Martinez, A. (2024, March 19). Apple's DMA compliance workshop—The power of no: Breaking apart the bundle? *Kluwer Competition Law Blog*. https://legalblogs.wolterskluwer.com/competition-blog/apples-dma-compliance-workshop-the-power-of-no-breaking-apart-the-bundle/

Roth, E. (2024a, January 25). Epic's Tim Sweeney calls Apple App Store changes 'hot garbage'. *The Verge*. https://www.theverge.com/2024/1/25/24050696/epic-games-tim-sweeney-apple-app-store-response

Roth, E. (2024b, January 26). Dirty tricks or small wins: Developers are skeptical of Apple's App Store rules. *The Verge*. https://www.theverge.com/24051818/apple-app-store-dma-eu-developer-response

Sorrel, C. (2026). Apple AirPods and malicious compliance. *IFIXIT*. https://www.ifixit.com/News/115572/apple-airpods-and-malicious-compliance#wppost-comments-container

Stigler, G. J. (1971). The theory of economic regulation. *The Bell Journal of Economics and Management Science*, *2*(1), 3–21. https://doi.org/10.2307/3003160

TikTok. (2026a). Digital Services Act transparency. *TikTok Safety*. https://www.tiktok.com/safety/en/transparency/dsa-transparency

TikTok. (2026b). European online safety. *TikTok*. https://www.tiktok.com/euonlinesafety/en/

TikTok. (2026c). How TikTok recommends content. *TikTok Help Center*. https://www.tiktok.com/support/faq_detail?id=7655285288050104852&category=web_account

Trans, M., Beraldo, D., Draisci, L., Afsahi, L., Brennan, M., Goldschmitt, V., Grendarova, T., Hamilton, H., Keskin, M., Papasokratous, M., Rossetti, G., Webb, M., Williams, J., & Xu, H. (2024). *APIcalypse now: Redefining data access regimes in the face of the Digital Services Act*. https://dare.uva.nl/id/6d4135e9-8ca5-4d4a-8da5-0537fa650337

Tzanaki, A., & Nowag, J. (2025). The institutional framework of the Digital Markets Act: A novel but thoughtful experiment in regulatory design? *Journal of European Competition Law & Practice*, *16*(7), 420–433. https://doi.org/10.1093/jeclap/lpag008

van de Kerkhof, J. (2025). Musk, techbrocracy, and free speech. *Verfassungsblog*. https://doi.org/10.59704/0db298323048f15a

Waldman, A. (2020). Privacy law's false promise. *Washington University Law Review*, *97*(3), 0773–0834.

Warzel, C. (2023, May 23). Twitter is a far-right social network. *The Atlantic*. https://www.theatlantic.com/technology/archive/2023/05/elon-musk-ron-desantis-2024-twitter/674149/

Weigl, L., Albert, J., & Pantic, S. (2026). *Unreasonable assurance: The auditing industry meets the DSA's systemic risk regime*.

X Corp. (2026). X transparency center. *X Transparency*. https://transparency.x.com/en

Yen, A. (2024, February 5). Apple's DMA compliance plan is a trap and a slap in the face for the European Commission. *Proton*. https://proton.me/blog/apple-dma-compliance-plan-trap

Published by

Alexander von Humboldt Institute for Internet and Society

CAIS Research for the Digital Age

in cooperation with

CREATe

cnrs centre internet et société

R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya

University of Tartu Johan Skytte Institute of Political Studies