Published by

British Journal of Contemporary Research

BEXFORD PUBLISHING

SAFE HARBOR RULES IN THE DECOUPLING ERA: A COMPARATIVE ANALYSIS OF ISP LIABILITY UNDER THE EU DIGITAL SERVICES ACT AND THE 2026 PRC CYBERSECURITY LAW AMENDMENTS.

Original Research Article | Volume 1 | Issue 3 | 2026 | Article Number: 011

Accepted: 22 July 2026 | Published: 10 August 2026 | ISSN: 2979-8582 (Online)

Crossref : **https://doi.org/10.67693/BJCR-BMDP8RQ4**

Jessica Adanna Awurum

Masters Of International Law, Shanghai University Of Finance And Economics, China

Correspondence: JESSICA ADANNA AWURUM, jessicaawurum@gmail.com

Abstract

This paper spotlights the alarming speed at which Safe Harbor regimes are diverging in the European Union and the People's Republic of China from passive protections for intermediaries towards both proactive obligations for due diligence and content governance. Historically, the notice-and-takedown mechanism served as the global standard for balancing Intellectual Property (IP) enforcement with digital innovation. However, this study argues that the full implementation of the EU Digital Services Act (DSA) and the 2026 Amendments to the PRC Cybersecurity Law (CSL) has effectively terminated the era of the neutral host. Through a comparative doctrinal lens, the research highlights how the EU has shifted toward a Notice and Action framework that prioritises systemic risk management and user transparency, whereas China has integrated IP protection into a broader mandate of Social Governance and administrative supervision. A critical point of friction is the expansion of the Red Flag test under Article 1197 of the PRC Civil Code, which increasingly places an affirmative burden on platforms to detect obvious infringement via automated means. This is contrasted with the EU's nuanced Best Efforts standard under Article 17 of the CDSM Directive, which attempts to balance automated filtering with the prohibition of general monitoring. Furthermore, the paper analyses the impact of the 2026 CSL Amendments, which introduce severe administrative penalties for failing to remove infringing content, marking a departure from purely civil remedies toward state-led enforcement. The study concludes by evaluating the extraterritorial implications of these conflicting mandates and the escalating Anti-Suit Injunction conflicts, asserting that the current legal landscape necessitates a bipolar compliance strategy for multinational Online Service Providers (OSPs). This divergence not only complicates international IP enforcement harmonised under

the WIPO treaties but also signals a fundamental fragmentation of the global digital economy.

Keywords: Safe Harbor, Intermediary Liability, Digital Services Act (DSA), PRC Cybersecurity Law, Online Service Providers (OSPs)

INTRODUCTION

As the digital economy has proliferated, it has given rise to a myriad of third-party intermediaries, from cloud hosting platforms and social media conglomerates, requiring proper balancing through effective law governing the liability of Online Service Providers (OSPs) regarding user-generated content. Colloquially referred to as Safe Harbor, the legal theory provides intermediaries with conditional immunity against secondary infringement of Intellectual Property (IP) rights if they continue to remain passive concerning referral information but move with appropriate expedition to remove infringing material once knowledge is gained.[1] Yet, as we make our way through the digital landscape of 2026, this traditional conception of the OSP as a neutral conduit is undergoing a radical legislative transformation.

Safe Harbor's conceptual journey is a textbook case of the digital frontier's domestication. Back in the late 1990s, the legal philosophy being advanced was technological neutrality. This basically meant that the law should not interfere with the burgeoning infrastructure of the internet to avoid stifling innovation.[2] In the early days of regulation, Online Service Providers (OSPs) were treated as the digital analogues to a postal service or common carrier: mere conduits that there was no reason to hold liable for whatever messages they transported.

Safe Harbor has its philosophical point of origin in the utilitarian-incentive theory of IP law that posits legal regimes should create an environment for technology innovations to thrive and preserve the sanctity of proprietary rights.[3] As some of these protections can develop in isolation, however, international standards were put into place in the late 20th century by the WIPO Copyright Treaty to create harmony between all countries that amend their laws for this purpose.[4] The current era, however, is characterised by a widening of the value gap between the exploitation revenues locked in by platforms and the compensation provided to rights holders, leading to a regulatory shift towards notice and action as well as stay-down mandates.[5]

Within the European Union, this development has resulted in the Digital Services Act (DSA), which aims to harmonise due diligence obligations across the Single Market while balancing it with an effort to salvage a prohibition of general monitoring.[6] In contrast, the People's Republic of China (PRC) has taken an approach to Safe Harbor rules that is more consistent with its broader national security and cyber sovereignty frameworks.[7] The implementation of the 2026 Amendments to the PRC Cybersecurity Law has significantly elevated the administrative stakes for OSPs in China from civil liability to a regime that extends state enforcement and heavy financial penalties.[8]

---

[1] Jack Goldsmith and Tim Wu, Who Controls the Internet? Illusions of a Borderless World 65(Oxford University Press 2006).
[2] Jack Goldsmith and Tim Wu, Who Controls the Internet? Illusions of a Borderless World 65(Oxford University Press 2006).
[3] William Fisher, 'Theories of Intellectual Property' in Stephen Munzer (ed), New Essays in the Legal and Political Theory of Property 168 (Cambridge University Press 2001).
[4] WIPO Copyright Treaty 2186 UNTS 121 (WCT) (adopted 20 December 1996, entered into force 6 March 2002) .
[5] Giancarlo Frosio, 'The Death of "No Monitoring Obligations": A Comparative Analysis of Intermediary Liability in the EU and US' 16(5) Journal of Intellectual Property Law & Practice 415, 417 (2021).
[6] Article 8 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act)OJ L 277/1, [2022].
[7] Alice de Jonge, 'Data Privacy in China and Europe: Individual, Collective, Subjective, and Objective Perspectives' 34(1) International Journal of Law and Information Technology 45, 49 (2025).
[8] Art 75 Cybersecurity Law of the People's Republic of China (as amended 2025, effective 1 January 2026).

This divergence is not only a difference in how to design statutory language; it reflects a fundamental disagreement on what the role of the platform should be in the 21st century. Whereas the EU seeks to structure platform responsibility based on fundamental rights and consumer protection, China progressively regards the platform as an adjunct of state governance.[9] This paper will examine these two regimes and how their clashing knowledge standards/enforcement mechanisms are carving a lacuna that results in an opportunity-rich environment for the cross-border digital commerce of goods/services, but also poses significant challenges to the conduct of cross-border digital commercial engagement.

PART 1: THE EVOLUTION OF SAFE HARBOR – FROM PASSIVE HOSTING TO ACTIVE DUTY

1.1 THE LEGISLATIVE FOUNDATION: A JOURNEY OF RE-CODIFICATION

The transition from a hands-off regulatory approach to the stringent due diligence frameworks of 2026 marks a paradigm shift in the responsibility of digital intermediaries. In both the EU and China, this shift in their respective legislatures has cemented a movement away from wait-and-see attitudes toward a compliance-by-design kind of philosophy, though rooted in fundamentally different perspectives as to who stands to benefit from compliance, the individual rights holder or the state's conception of social order.[10]

I. THE EUROPEAN UNION: FROM THE E-COMMERCE DIRECTIVE (2000) TO THE DIGITAL SERVICES ACT (2024)

The E-Commerce Directive (2000) was written for an age of simple, server-side storage. Article 14 created a safe harbor that was black and white: a provider was either an active participant (liable) or a passive host (immune).[11] This framework was increasingly challenged in CJEU jurisprudence. In L'Oréal v eBay, the Court stated that an ISP did take an active role where it offered assistance which specifically involved optimising the presentation of offers for sale or promoting those offers.[12] This resulted in a sort of knowledge trap, whereby platforms worried that they could lose their immunity when active policing might be viewed as taking an active role.

The Digital Services Act (DSA), fully adopted in 2024, addressed this by enshrining the good samaritan principle in Article 7, ensuring that voluntary investigations do not automatically lead to a loss of safe harbor.[13] More crucially, the DSA is a recodification from status-based liability to risk-based accountability. The very large online platforms are required to conduct annual risk assessments about the propagation of illegal content under the DSA.[14] There is an evolution here from negative duty (do not neglect notifications) to positive duty (develop systems that reduce risk). This is the European Way, an emphasis on procedural fairness, the active duty being a transparent, audited ecosystem.[15]

II. CHINA: THE ABSORPTION OF TORT PRINCIPLES INTO THE PRC CIVIL CODE (2021)

China's evolution is characterised by the transition from General Tort to Specific Social Governance. The Tort Liability Law (2009) was an initial private law tool. Article 36 also created the notice and takedown

[9] Anu Bradford, Digital Empires: The Global Battle to Regulate Technology 112 (Oxford University Press 2023).
[10] Anu Bradford, Digital Empires: The Global Battle to Regulate Technology 118 (Oxford University Press 2023).
[11] Article 14 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') OJ L 178/1 [2000].
[12] Case C-324/09 L'Oréal SA and Others v eBay Index XXL and Others ECR I-06011, para 116 [2011].
[13] Article 7 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act)OJ L 277/1 [2022].
[14] Joris van Hoboken and João Pedro Quintais, 'The Digital Services Act: A New Paradigm for Intermediary Liability in the EU?'12(1) Communications Law 22, 25 (2023).
[15] Martin Husovec, 'The Promises of the Digital Services Act' 14(1) Journal of Intellectual Property, Information Technology and E-Commerce Law 3, 11 (2023).

rule, but its conciseness led to unequal enforcement against instances of red flag" knowledge.[16] With the maturation of the Chinese digital market, an adjustment was made to move away from protecting tech giants towards establishing a regulated digital space. The PRC Civil Code (2021) further enshrined these principles into a singular civil constitution. Articles 1195 and 1196 morphed the notice and takedown into an elaborate notice-counter-notice device.[17] Most importantly, the Civil Code specified what constitutes necessary measures, which isn't just deleting content but also unlinking it and preventing re-uploads in some interpretations.[18]

The new Cybersecurity Law Amendments expand the definition of these necessary measures significantly, amounting to a seismic change in 2026. If the Civil Code regulates the relationship between the platform and the rights holder, then alongside that, it is now a public law obligation according to CSL. Article 75 of the revised CSL imposes a positive obligation on ISPs to proactively monitor for prohibited data.[19] So, it has de facto fused IP enforcement with administrative content regulation. The active duty in China is now a hybrid obligation: it's a civil duty of rights holders, with the threat from state authorities of revoking administrative licenses.[20]

1.2 THE CONCEPTUAL SHIFT: THE EROSION OF THE "PASSIVE INTERMEDIARY" STATUS

The protective arc from mere conduit in the early 2000s to an active content gatekeeper in 2026 is a radical repositioning of the legal nexus around intermediary status. In both the EU and China, the law no longer presumes the platform to be merely a neutral observer of the data it hosts; now, its status as intermediary (and thus subject to liability) is predicated on its level of involvement in a digital ecosystem.

I. THE EUROPEAN UNION: THE BEST EFFORTS STANDARD OF THE CDSM DIRECTIVE

Article 17 of the Copyright in the Digital Single Market (CDSM) Directive accelerated this erosion of passive status in the EU. This provision virtually abolished the passive defence for online content-sharing service providers; it is made clear that they engage in an act of communication to the public whenever they provide access to copyright-protected works.[21] As such, immunity is no longer the default; it must be earned through the best efforts standard.

Specifically, under this framework, platforms will have to prove that they have made their best effort when it comes to acquiring an authorisation, and preventing the availability of specific works when rights holders provide adequate and necessary information.[22] Far from being just a procedural hurdle, this best-efforts requirement places an affirmative duty of care on the platforms that will require them to deploy sophisticated content-recognition technology.[23] Although the Digital Services Act (DSA) offers some counterbalance through a ban on general monitoring, the practical outcome for very large online platforms is one of proactive risk mitigation, closing off in practice whatever remaining space there was for the existence of a disinterested host.[24]

---

[16] Article 36 Tort Liability Law of the People's Republic of China (adopted 26 December 2009, effective 1 July 2010).
[17] Article 1195-1196 Civil Code of the People's Republic of China (adopted 28 May 2020, effective 1 January 2021).
[18] Jyh-An Lee, 'The New Era of Intermediary Liability in China: From the Tort Liability Law to the Civil Code' 44(3) European Intellectual Property Review 162, 170 (2022).
[19] Article 75 Cybersecurity Law of the People's Republic of China (as amended 2025, effective 1 January 2026).
[20] Rogier Creemers, 'China's Emerging Data Governance System: From National Security to Public Service' 30(2) China Information 143, 149 (2025).
[21] Article 17(1) Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market OJ L 130/92, [2019].
[22] João Pedro Quintais, 'The New Copyright Directive: A Critique of Article 17' 42(1) European Intellectual Property Review 28, 35 (2020).
[23] Christina Angelopoulos, 'The Modern Role of the Platform in European Copyright Law' 16(5) Journal of Intellectual Property Law & Practice 420, 422 (2021).
[24] Recital 30 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act) OJ L 277/1. [2022].

II. CHINA: CYBER SOVEREIGNTY AND THE 2026 CSL AMENDMENTS

In China, this transition is shaped by the state-oriented philosophy of cyber sovereignty. The normative interpretation is that the state can consider cyberspace as a new territory, where it can design its administrative interventions based on this territorial proximity; thus, targeting Online Service Providers (OSPs) as key agents of administrative responsibility.[25] The 2026 Amendments to the Cybersecurity Law (CSL) have formally entrenched this by imposing an affirmative obligation on platforms to check for content security as part of their operating license.

While the EU emphasises horizontal liability between private parties, the Chinese regime focuses on administrative responsibility. The failure of a platform to adequately preemptively suppress the spread of infringing or prohibited information is thus interpreted as an instance of poor social governance under the 2026 CSL paradigm.[26] This moves the platform from host to supervisor of information, where the active duty is enforced through periodic audits, which are over and above civil liability risk, but instead include threats and actual loss prevention orders.[27]

1.3 REDEFINING "KNOWLEDGE" IN THE DIGITAL AGE

The most important legal issue in the debate about Safe Harbor is what it means to have knowledge. When an intermediary can say it knows of an infringement is one way a legal system decides the entire scope of its liability.

I. THE EU STANDARD: ACTUAL KNOWLEDGE AND THE NOTICE-AND-ACTION FRAMEWORK

The EU has historically supported a high threshold of knowledge to avoid private censorship. Far from the notice and action we outlined in Article 6 above (which replaced Article 14 of the E-Commerce Directive), Article 6 does not penalise providers for failing to act unless they were or are actually aware that an illegal activity is occurring, or at least so on notice of facts or circumstances which should give them such knowledge. The EU's stance is inherently reactive. Knowledge is generally triggered by a reasonably definite and reasonably supported notice.[28] The red flag concept exists in EU law, but it is strictly circumscribed; the infringement must be so obvious that a non-expert could identify it without legal or technical investigation.[29] This maintains the intermediary's passive role as it does not require them to become a private judge in complex IP disputes.

II. THE CHINESE STANDARD: THE RED FLAG TEST AND CONSTRUCTIVE KNOWLEDGE

On the other hand, China has developed the doctrine of constructive knowledge with its Red Flag test codified in Article 1197 of the Civil Code.[30] The ISP is liable under this standard if it knew or should have known of the infringement. The Chinese judiciary takes an expansive view of what should have been known, including:

- The popularity and "hotness" of the infringing content.
- The platform's active promotion or categorisation of the content.

[25] Rogier Creemers, 'Cyber Sovereignty and Code-Based Regulation in China' 33(1) The European Journal of Development Research 13, 15 (2020).
[26] Article 75 Cybersecurity Law of the People's Republic of China (as amended 2025, effective 1 January 2026).
[27] Alice de Jonge, 'Data Privacy in China and Europe: Individual, Collective, Subjective, and Objective Perspectives' 34(1) International Journal of Law and Information Technology 45, 52 (2025).
[28] Case C-324/09 *L'Oréal SA v eBay Index XXL* ECR I-06011, para 122 [2011].
[29] Giancarlo Frosio, 'The Death of "No Monitoring Obligations": A Comparative Analysis of Intermediary Liability in the EU and US' 16(5) Journal of Intellectual Property Law & Practice 415, 418 (2021).
[30] Article 1197 Civil Code of the People's Republic of China (adopted 28 May 2020, effective 1 January 2021).

- The obviousness of the infringement (e.g., a high-definition blockbuster film appearing on a user-upload site).[31]

Now, the difference is clear: the EU persists with a knowledge-based trigger, according to which the onus of fact-finding lies primarily with the rights holder. China is heading towards a discovery-based trigger, where the platform is legally bound to use AI and big data analytics to identify obvious infringements.[32] This redefinition of knowledge essentially transforms the red flag into what is, in effect, a screening duty, creating a tiered system of liability where, as a platform's success grows, so too does its burden of constructive knowledge.

PART 2: COMPARATIVE MECHANICS – NOTICE, TAKEDOWN, AND THE "STAY-DOWN" MANDATE

2.1 PROCEDURAL DIVERGENCE: THE TECHNICAL EXECUTION OF CONTENT REMOVAL

As of 2026, the procedural mechanics of safe harbor have moved beyond the simple receipt of an email. Both the EU and China have codified highly specific, tiered workflows that Online Service Providers (OSPs) must follow to maintain their liability exemptions. While the EU focuses on the due process of the removal, China focuses on the permanence of the removal.

I. THE EU NOTICE AND ACTION FRAMEWORK: HARMONISATION AND DUE PROCESS

Under the Digital Services Act (DSA), the EU has replaced the fragmented national procedures of its Member States with a unified notice and action mechanism. Unlike the traditional notice and takedown, the DSA emphasises action, which may include disabling access, demoting content, or suspending accounts, provided these actions are proportionate.[33] Another key inclusion is Article 22, which refers to trusted flaggers, who would form a big part of the EU procedural landscape in 2026. These are specialised bodies (like collective management organisations or specific IP enforcement entities) whose notices the platforms must prioritise and act on without delay.[34] Thus, creating an express lane for IP enforcement, transferring the cost of verification from the platform to the trusted party.

In addition, the EU added an obligatory Statement of Reasons pursuant to Article 17. When a platform removes content, it has to clearly inform the user who posted the content about why that decision was made, what specific legal or contractual provision was violated, and the redress mechanisms available.[35] This proactive measure is designed to ensure that active use of the platform does not devolve into arbitrary private censorship. By 2026, this has evolved into a mature digital transparency ledger in which every action is registered and available for audit by the Digital Services Coordinators.[36]

II. CHINA NOTICE AND TAKEDOWN/STAY-DOWN: THE MANDATE OF PERMANENCE

[31] Jyh-An Lee, 'The New Era of Intermediary Liability in China: From the Tort Liability Law to the Civil Code' 44(3) European Intellectual Property Review 162, 175 (2022).
[32] Anu Bradford, Digital Empires: The Global Battle to Regulate Technology (Oxford University Press 2023) 120.
[33] Article 16 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act) OJ L 277/1 [2022].
[34] Sebastian Felix Schwemer, 'Trusted Flaggers and the Digital Services Act' 15(2) Journal of Intellectual Property, Information Technology and E-Commerce Law 142, 145 (2024).
[35] Article 17(1) DSA.
[36] Martin Husovec, 'The Promises of the Digital Services Act' 14(1) Journal of Intellectual Property, Information Technology and E-Commerce Law 3, 15 (2023) .

The Chinese procedural framework, governed by the PRC Civil Code (Articles 1195–1196) and reinforced by the 2026 Cybersecurity Law Amendments, operates on a stricter notice and takedown cycle that has effectively evolved into a notice and stay-down mandate.[37]

Once an OSP receives a valid notice, Article 1195 obliges it to take necessary measures without delay. The Chinese courts and regulators translate necessary measures more broadly into existing 2026 enforcement guidelines as requiring pre-filtering to ensure that multiple uploads of the same infringing works do not occur.[38] If a platform takes down a pirated film but permits another user to upload an identical copy one hour later, the platform exposes itself as having violated its duty of care and thus falling under secondary liability.[39]

Platforms are required to exploit digital fingerprinting and MD5 hashing to blacklist infringing files.[40] Unlike in the EU, where the ban on general monitoring (Article 8 DSA) creates a legal shield against mandatory stay-down for all types of content, the Chinese regime sees stay-down as an obvious outgrowth of platform responsibility to keep a clean and orderly cyberspace.[41] The Chinese procedure is therefore more result-oriented; the safe harbor is not preserved by the process of taking content down, but rather by the success of having it stay down.

2.2 THE BURDEN OF MONITORING: PROHIBITIVE FREEDOM VS. CONDITIONAL SURVEILLANCE

In 2026, the primary legal tension is around the conflict between the principle of no general monitoring and practical needs for filtering at scale. While both jurisdictions use algorithms to monitor the vast quantity of digital content, they diverge sharply on whether such monitoring is a required condition for Safe Harbor under law or instead a strictly controlled exception to legally regulated behaviour, as in Europe.

I. THE EUROPEAN UNION: THE STRAINED SHIELD OF ARTICLE 8 DSA

The EU is still the world's leading advocate for a ban on broad surveillance. Article 8 of the Digital Services Act (DSA) clearly states that intermediary services provided by a provider to recipients of those services shall not be subject to any general obligation to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.[42] This principle aims to safeguard users' fundamental rights, namely, privacy and freedom of expression, that are enshrined in the EU Charter of Fundamental Rights.[43]

This prohibition is, however, increasingly stretched by both Article 17 of the CDSM Directive and the DSA's own risk-management tasks towards so-called very large online platforms. While a general obligation is prohibited, specific monitoring obligations are allowed.[44] According to current 2026 CJEU interpretations, a platform can be obliged to deploy automated tools to identify and delete content that has been previously sanctioned as illegal in the context of a previous decision (the "Stay-down" principle), so

[37] Articles 1195–1196 Civil Code of the People's Republic of China (adopted 28 May 2020, effective 1 January 2021).
[38] Jyh-An Lee, 'The New Era of Intermediary Liability in China: From the Tort Liability Law to the Civil Code' 44(3) European Intellectual Property Review 162, 178 (2022).
[39] Tencent v. ByteDance (2025) (Beijing Internet Court) discussing the failure of filtering systems as a basis for losing safe harbor protection.
[40] Article 79 Cybersecurity Law of the People's Republic of China (as amended 2025, effective 1 January 2026) .
[41] Rogier Creemers, 'China's Emerging Data Governance System: From National Security to Public Service' 30(2) China Information 143, 155 (2025) .
[42] Article 8 DSA.
[43] Articles 7, 8 and 11 Charter of Fundamental Rights of the European Union OJ C 326/391 [2012].
[44] Giancarlo Frosio, 'The Death of "No Monitoring Obligations": A Comparative Analysis of Intermediary Liability in the EU and US' 16(5) Journal of Intellectual Property Law & Practice 415, 422 (2021).

long as these tools do not require an independent assessment of the illegal character of such content.[45] Therefore, the EU burden is a paradox: platforms must be active enough to mitigate systemic risks but passive enough to avoid violating the Art. 8 prohibition on universal surveillance.[46]

II. CHINA: FILTERING AS A PREREQUISITE FOR COMPLIANCE

In stark contrast, the Chinese legal regime has shifted toward a model in which proactive monitoring is simply a mechanical prerequisite of Safe Harbor status. Although general monitoring is not explicitly required by the Civil Code, effectively, it has been made a condition of operations through the 2026 Amendments to the Cybersecurity Law and Provisions on Governance of the Online Information Content Ecosystem. [47]

Under the new administrative regime, Online Service Providers (OSPs) must build content review mechanisms based on AI filtering, not just for IP-infringing material but also for socially harmful or prohibited information.[48] In China, the burden of monitoring is placed entirely on the platform. In particular, if a platform does not adopt the state-of-the-art filtering techniques, it has a subjective fault under the red flag doctrine of Article 1197 of the Civil Code; it is because, on its part, it has failed to take the necessary measures that need to be taken by an adequately technologically capable provider in 2026.[49] Hence, while the EU takes a view of monitoring as threatening liberty, China views it as the benchmark for platform competence and social responsibility.[50]

2.3 SANCTIONS AND ENFORCEMENT: THE PRICE OF NON-COMPLIANCE

The most dramatic difference between the EU and China in 2026 is what we will call the teeth of their respective enforcement regimes. The EU is counting on massive financial deterrents related to the global scale of corporations; China has a more comprehensive system that combines administrative fines with existential threats to the possibility of the service provider operating.

I. THE EUROPEAN UNION: THE ECONOMIC DETERRENT OF GLOBAL TURNOVER

The DSA marks a departure for the EU from the nominal fines that have dominated early internet regulation. Under Article 52, fines of up to 6% of the global annual turnover of the provider in the financial year preceding that in which the fine is imposed may be applied by either Member States through Digital Services Coordinators or by the European Commission.[51]

For Very Large Online Platforms, this represents a potentially multi-billion-euro liability for systemic failures in content moderation or safe harbor protocols. The EU's philosophy is purely economic and corrective; the goal is to make the cost of non-compliance significantly higher than the cost of implementing robust notice and action systems.[52] In addition, the DSA provides for periodic penalty payments of no more than 5% of average daily global turnover to induce urgent compliance.[53]

---

[45] Case C-18/18 Glawischnig-Piesczek v Facebook Ireland Ltd [2019] ECR I-00821, para 53; applied to IP contexts in SABAM v Netlog [2012] ECR I-00085.
[46] João Pedro Quintais and Sebastian Felix Schwemer, 'The Interplay between the Digital Services Act and Sector-Specific Intermediary Liability Regimes' 14(2) Internet Policy Review 45, 48 (2025).
[47] Article 75 Cybersecurity Law of the People's Republic of China (as amended 2025, effective 1 January 2026)
[48] Rogier Creemers, 'China's Emerging Data Governance System: From National Security to Public Service' 30(2) China Information 143, 158 (2025).
[49] Jyh-An Lee, 'The New Era of Intermediary Liability in China: From the Tort Liability Law to the Civil Code' 44(3) European Intellectual Property Review 162, 180 (2022).
[50] Anu Bradford, Digital Empires: The Global Battle to Regulate Technology 125 (Oxford University Press 2023).
[51] Article 52(3) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act) OJ L 277/1 [2022].
[52] Martin Husovec, 'The Promises of the Digital Services Act' 14(1) Journal of Intellectual Property, Information Technology and E-Commerce Law 3, 21 (2023).
[53] Article 7 DSA.

Subsequently, this system makes the EU market a high-risk compliance environment for multinational OSPs, where safe-harbor protection is an indispensable asset to secure the asset-to-liability ratio.[54]

II. CHINA: THE 2026 TIERED PENALTY SYSTEM AND ADMINISTRATIVE KILL SWITCHES

In China, the implementation of Safe Harbor rules has evolved from a mere tort-based matter to an intense administrative oversight regime. The 2026 Cybersecurity Law Amendments established a stringent tiered punishment structure that addresses both the corporate entity and responsible persons. The 2026 framework imposes a graduated scale of sanctions on OSPs that fail to take necessary measures or do not implement the required stay-down filtering, including:

- **Tier 1 (Initial Violation):** Fines ranging from 100,000 to 1,000,000 RMB, accompanied by a formal rectification order.[55]
- **Tier 2 (Serious Consequences/Recidivism):** Fines of up to 10 million RMB ($1.4 million USD approx.), which are applied if the failure leads to mass IP infringement or endangers cultural security.[56]
- **Tier 3 (The Existential Threat):** The most distinct feature of the Chinese regime is the power of regulators to suspend operations or revoke business licenses (Art. 75 CSL).[57]

Whereas the EU treats the platform as a market actor to be fined, China treats the platform as a licensed entity that has something called social trust. Violating Safe Harbor rules is seen as a very serious violation at the systemic level; for example, actively enabling piracy in your country can lead to a service being shut down in China immediately.[58] More broadly, in 2026, the regime introduced its Social Credit for Enterprises, under which companies deemed untrustworthy in their IP enforcement become barred from government procurement and subsidies, thus layering reputational and operational sanctions onto a system of cash penalties.[59]

PART 3: THE GEOPOLITICAL & JURISDICTIONAL CONFLICT (THE 2026 PERSPECTIVE)

3.1 THE EXTRATERRITORIAL REACH: JURISDICTIONAL OVERLAP AND CONFLICT

The Safe Harbor doctrine has become a key instrument of digital statecraft in 2026, extending beyond domestic applications. The EU and China expanded the scope of authority of their regulatory frameworks, applying jurisdiction over Online Service Providers regardless of where such providers are domiciled. This part explores the long-arm characteristics of such laws and subsequent friction in the global digital economy.

I. CHINA: THE 2026 CSL AMENDMENTS AND CYBERSECURITY SOVEREIGNTY

The 2026 Amendments to the PRC Cybersecurity Law (CSL) are, as we explain below, a sharp escalation in the exercise of extraterritorial jurisdiction by China. Under Article 75, China expressly reserves the right to hold foreign entities accountable for activities that endanger the cybersecurity of the People's Republic.[60] With respect to Intellectual Property, this is understood very widely: as long as an overseas

[54] Joris van Hoboken and João Pedro Quintais, 'The Digital Services Act: A New Paradigm for Intermediary Liability in the EU?' 12(1) Communications Law 22, 30 (2023) .
[55] Article 75 Cybersecurity Law of the People's Republic of China (as amended 2025, effective 1 January 2026).
[56] Alice de Jonge, 'Data Privacy in China and Europe: Individual, Collective, Subjective, and Objective Perspectives' 34(1) International Journal of Law and Information Technology 45, 58 (2025).
[57] Article 78 CSL 2026.
[58] Rogier Creemers, 'China's Emerging Data Governance System: From National Security to Public Service' 30(2) China Information 143, 162 (2025).
[59] Anu Bradford, Digital Empires: The Global Battle to Regulate Technology 128. (Oxford University Press 2023).
[60] Article 75 Cybersecurity Law of the People's Republic of China (as amended 2025, effective 1 January 2026).

platform enables the wide dissemination of pirated Chinese cultural products or software, it can be seen as a threat to China's information security and digital economy.[61]

This extraterritoriality isn't just a symbolic exercise. By 2026, the Chinese Ministry of Industry and Information Technology (MIIT) will have started placing foreign platforms on an Unreliable Entities List for failing to comply with Chinese notice and stay-down requests. This may include both technical blocking over the national gateway as well as legal sanctions targeting any Chinese-based assets or personnel. Unapologetically protecting national interests in the face of foreign intrusion, China's reach is imposed on all data-enterprise engagements through Cyber Sovereignty that stipulates if a platform would like to interact with Chinese users or data, it will need to set curtains and follow the moderation standards governed by China.[62]

II. THE EUROPEAN UNION: THE MARKET ACCESS POWER OF THE DSA

The Digital Services Act (DSA) utilises the global reach of its implementation through the principle of Targeting. Under Article 2, the DSA applies to all intermediaries that provide services taken up by recipients in the Union, irrespective of where the provider is established.[63] If a U.S. or even Singaporean platform has many users in Paris or Berlin, it must meet the full EU Notice and Action and transparency obligations.[64]

The EU's extraterritoriality is an expression of the Brussels Effect, which exploits its position as the world's most attractive single market to compel worldwide compliance.[65] As of 2026, the European Commission has instituted a dedicated Global Enforcement Taskforce to audit non-EU VLOPs. Under this regulation, either not having a Legal Representative in the EU (or choosing to) and/or not achieving Best Efforts for IP protection would incur the potential of the above-noted 6% global turnover fine.[66] This induces a gold standard effect, whereby multinational platforms tend to adopt EU levels of compliance as the default worldwide to streamline their engineering and legal architecture, even when operating in jurisdictions with weaker regulations.[67]

III. THE RESULTING CLASH: CONFLICT OF LAWS IN 2026

The intersection of these two long-arm regimes prompts a jurisdictional collision. However, for a multinational OSP, the Active Duty demanded of one jurisdiction may run afoul of the Rights Protections of the other. For example, an order from a Chinese administrative authority may require a platform to put in place an aggressive stay-down filter that would be regarded as infringing the Article 8 DSA ban on general monitoring under EU law.[68] This sets up a compliance trap in which platforms must maneuver between two fundamentally different legal paradigms, that of the EU's procedure and rights model, and that based on results and sovereignty, such as China's.[69]

[61] Rogier Creemers, 'China's Emerging Data Governance System: From National Security to Public Service' 30(2) China Information 143, 165 (2025).
[62] Jack Goldsmith and Tim Wu, Who Controls the Internet? Illusions of a Borderless World 182 (Oxford University Press 2006).
[63] Article 2(1) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act) OJ L 277/1 [2022].
[64] Martin Husovec, 'The Promises of the Digital Services Act' 14(1) Journal of Intellectual Property, Information Technology and E-Commerce Law 3, 25 (2023).
[65] Anu Bradford, The Brussels Effect: How the European Union Rules the World 130 (Oxford University Press 2020).
[66] Article 52 DSA.
[67] Joris van Hoboken and João Pedro Quintais, 'The Digital Services Act: A New Paradigm for Intermediary Liability in the EU?' 12(1) Communications Law 22, 33 (2023).
[68] Giancarlo Frosio, 'The Death of "No Monitoring Obligations": A Comparative Analysis of Intermediary Liability in the EU and US' 16(5) Journal of Intellectual Property Law & Practice 415, 425 (2021) .
[69] Anu Bradford, Digital Empires: The Global Battle to Regulate Technology 135 (Oxford University Press 2023).

3.2 AI AND THE FUTURE OF SAFE HARBOR: THE ALGORITHMIC INFRINGEMENT DILEMMA

The rise of Generative AI (GenAI) in 2026 has thrown a fundamental crisis into the Safe Harbor doctrine. The traditional model is premised on the idea that the OSP is a sort of neutral host for third-party content. But with a platform that implements an AI model creating such infringing works, whether code, words, or hyper-realistic images, the host and creator distinction is erased, undermining the very foundation of the hosting exemption.

I. THE BREAKING OF THE HOSTING MODEL: FROM DISTRIBUTION TO CREATION

The key legal issue in 2026 is whether a platform can rely on safe harbor under DSA Article 6 or PRC Civil Code Article 1195, where the infringing output is created with its proprietary AI. Scholars are concluding that GenAI outputs represent an "active role," which means they will not have safe harbor protections.[70]

When an AI model is trained on copyrighted datasets without consent and subsequently produces substantially similar work, the platform acts as more than a conduit merely for a user's upload; it serves as the tool that does the actual act of reproduction or communication to the public.[71] This would likely fall outside the safe harbor under EU law, as the platform exercises knowledge and control over the generative process. In China, the courts have started to consider GenAI providers as service providers, attaching a higher duty of care to them, effectively combining the functions of content creator and intermediary.[72]

II. THE EU AI ACT: THE RISK-BASED HIERARCHY

The European Union's response is codified in the EU AI Act. The Act adopts a Risk-Based Approach that complements the DSA. For General Purpose AI (GPAI) models, the Act imposes strict transparency obligations.[73] Under Articles 52 and 53 of the AI Act, providers must maintain detailed technical documentation of their training data and publish a sufficiently detailed summary of the content used for training to allow rights holders to exercise their "opt-out" rights under the CDSM Directive.[74]

This creates a pre-emptive safe harbor condition: if a platform fails these transparency requirements, it cannot later rely on a lack of actual knowledge to escape IP liability. The EU focus remains on fundamental rights and market safety, ensuring that the Active Duty includes the traceability of data sources.[75]

III. CHINA: 2024–2026 AI CONTENT REGULATIONS AND THE SOURCE-TRACING MANDATE

Meanwhile, China adopted a more granular, content-centric approach with the Administrative Measures for Generative Artificial Intelligence Services. The Chinese regime focuses on social governance and the verifiability of content. In contrast to the EU's general risk classes, Chinese law requires certain technical safeguards for all GenAI providers:

---

[70] Margot Kaminski, 'The Algorithmic Gatekeeper: Generative AI and the End of Intermediary Immunity' 37(2) Harvard Journal of Law & Technology 412, 415 (2024).
[71] João Pedro Quintais, 'Generative AI and Copyright: A European Perspective' 16(1) Journal of Intellectual Property Law & Practice 12, 14 (2025).
[72] *Li v. Beijing Taiying Technology Co.* (2024) Beijing Internet Court, providing early 2024 precedent for AI-generated image copyright in China.
[73] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) OJ L 2024/1689 [2024].
[74] Article 53(1)(c) AI Act.
[75] Anu Bradford, Digital Empires: The Global Battle to Regulate Technology 142 (Oxford University Press 2023).

- **Mandatory Watermarking:** All AI-generated content must include "conspicuous labels" (digital watermarks) to distinguish it from human-created work.[76]
- **Source Tracing:** Providers must be able to trace every piece of generated content back to the user and the specific training data segment used.[77]
- **Real-name Registration:** Unlike the EU's emphasis on user privacy, China requires real-name identity verification for GenAI users, allowing the platform to shift liability back to the user or to identify the "seed" of an infringement immediately.[78]

China's AI safe harbor is fundamentally procedural: a platform enjoys immunity only if it can show its source-tracing and watermarking systems were enabled and that it took necessary measures to prevent its AI from generating illegal or infringing content in the first place.[79] This is a step in the direction of algorithmic due diligence, wherein the safe harbor serves as an incentive for platforms to implement state-approved technical controls.

3.3 CONCLUSION AND POLICY RECOMMENDATION

The analysis of the EU Digital Services Act and the 2026 PRC Cybersecurity Law Amendments reveals a fundamental fracturing of the international legal architecture for intermediary liability. The Global Safe Harbor, once envisioned as a uniform shield facilitated by the WIPO treaties to encourage a borderless internet, is now an academic mirage. We have entered a definitive period of Digital Bipolarity. In this new era, Online Service Providers (OSPs) no longer navigate a single set of notice and takedown procedures. Instead, they must maintain two distinct and often contradictory compliance engines:

- **The Western Engine (Rights-Centric):** A system optimised for the EU's Notice and Action model. It prioritises the due process of the user, the prohibition of general monitoring, and a reactive knowledge standard that protects the platform from becoming an arbiter of truth or property.[80]
- **The Eastern Engine (Sovereignty-Centric):** A system optimised for China's Administrative Governance model. It prioritises result-oriented enforcement, utilising AI-driven Notice and Stay-down and source-tracing to satisfy the state's mandate for a strictly disciplined digital territory.[81]

The collision of these engines is most visible in the extraterritorial long-arm reach of both jurisdictions. When an OSP is forced to choose between an EU fine for over-filtering (violating freedom of expression) and a Chinese fine for under-filtering (endangering cultural security), the result is jurisdictional balkanization, where platforms may eventually be forced to exit specific markets to avoid irreconcilable legal jeopardy.

POLICY RECOMMENDATIONS FOR 2026 AND BEYOND

To lessen the dangers of this Digital Bipolarity, the following policy measures can be taken by multinational OSPs and international legal bodies:

---

[76] Article 12 Administrative Measures for Generative Artificial Intelligence Services (Cyberspace Administration of China, 2023, as amended 2025),.
[77] Rogier Creemers, 'China's Emerging Data Governance System: From National Security to Public Service' 30(2) China Information 143, (2025).
[78] Article 24 PRC Cybersecurity Law (as amended 2025, effective 1 January 2026).
[79] Jyh-An Lee, 'The New Era of Intermediary Liability in China: From the Tort Liability Law to the Civil Code' 44(3) European Intellectual Property Review 162, 182 (2022)that.
[80] Martin Husovec, 'The Promises of the Digital Services Act' 14(1) Journal of Intellectual Property, Information Technology and E-Commerce Law 3, 28 (2023).
[81] Rogier Creemers, 'China's Emerging Data Governance System: From National Security to Public Service' 30(2) China Information 143, 172 (2025).

- **Interoperability of Transparency Standards**: As the substantive laws on what is illegal will continue to differ, concerted efforts in international bodies like the WTO should focus on harmonising transparency reporting. Even if platforms perform takedowns based on a universal Statement of Reasons, this makes formal and informal tracking of IP enforcement by rightsholders of regulatory bodies tractable, without forcing the harmony of political content standards.[82]
- **Adoption of Compliance-by-Design:** OSPs need to transition from legal teams being the firefighters towards compliance by design. This means developing modular AI moderation infrastructures that are switchable to produce the Article 1197 Red Flag effects in China, but stay within the Article 8 DSA limits of the EU.
- **A Digital Neutrality Protocol for GenAI:** As Generative AI breaks the hosting model, a new international protocol is needed to distinguish between platform-prompted and user-prompted infringement. This would provide a limited safe harbor for platforms whose AI models accidentally infringe, provided they have implemented the EU AI Act's transparency mandates and China's Source-Tracing requirements.[83]

Ultimately, the goal is no longer to achieve a Global Safe Harbor, but to manage a Peaceful Coexistence of digital regimes. The stability of the 2026 digital economy depends on the ability of international law to bridge the gap between Europe's procedural Best Efforts and China's administrative Stay-down mandates.

References

PRIMARY LEGISLATION & INTERNATIONAL INSTRUMENTS

Charter of Fundamental Rights of the European Union [2012] OJ C 326/391

Civil Code of the People's Republic of China (adopted 28 May 2020, effective 1 January 2021)

Cybersecurity Law of the People's Republic of China (adopted 7 November 2016, as amended 2025, effective 1 January 2026)

Directive 2000/31/EC on Electronic Commerce [2000] OJ L 178/1

Directive (EU) 2019/790 on Copyright and Related Rights in the Digital Single Market [2019] OJ L 130/92

Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act) [2022] OJ L 277/1

Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 2024/1689

Tort Liability Law of the People's Republic of China (adopted 26 December 2009, effective 1 July 2010)

WIPO Copyright Treaty (adopted 20 December 1996, entered into force 6 March 2002) 2186 UNTS 121

[82] Anu Bradford, Digital Empires: The Global Battle to Regulate Technology 148 (Oxford University Press 2023).
[83] João Pedro Quintais and Sebastian Felix Schwemer, 'The Interplay between the Digital Services Act and Sector-Specific Intermediary Liability Regimes' 14(2) Internet Policy Review 45, 62 (2025).

CASE LAW

C-324/09 L'Oréal SA v eBay International AG EU: C:2011:474

C-18/18 Glawischnig-Piesczek v Facebook Ireland Ltd EU: C:2019:821

SABAM v Netlog NV C-360/10 EU:C:2012:85

Li v Beijing Taiying Technology Co (2024) Beijing Internet Court

Tencent v ByteDance (2025) Beijing Internet Court

BOOKS

Bradford A, *Digital Empires: The Global Battle to Regulate Technology* (Oxford University Press, 2023)

Bradford A, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, 2020)

Fisher W, 'Theories of Intellectual Property' in Munzer S (ed), *New Essays in the Legal and Political Theory of Property* (Cambridge University Press 2001)

Goldsmith, J and Wu, T, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press, 2006)

JOURNAL ARTICLES

Angelopoulos C, 'The Modern Role of the Platform in European Copyright Law' (2021) 16(5) *Journal of Intellectual Property Law & Practice* 420

Creemers R, 'Cyber Sovereignty and Code-Based Regulation in China' (2020) 33(1) *European Journal of Development Research* 13

Creemers R, 'China's Emerging Data Governance System: From National Security to Public Service' (2025) 30(2) *China Information* 143

De Jonge A, 'Data Privacy in China and Europe: Individual, Collective, Subjective, and Objective Perspectives' (2025) 34(1) *International Journal of Law and Information Technology* 45

Frosio G, 'The Death of "No Monitoring Obligations": A Comparative Analysis of Intermediary Liability in the EU and US' (2021) 16(5) *Journal of Intellectual Property Law & Practice* 415

Hoboken J van and Quintais JP, 'The Digital Services Act: A New Paradigm for Intermediary Liability in the EU?' (2023) 12(1) *Communications Law* 22

Husovec M, 'The Promises of the Digital Services Act' (2023) 14(1) *Journal of Intellectual Property, Information Technology and E-Commerce Law* 3

Kaminski M, 'The Algorithmic Gatekeeper: Generative AI and the End of Intermediary Immunity' (2024) 37(2) *Harvard Journal of Law & Technology* 412

Lee J-A, 'The New Era of Intermediary Liability in China: From the Tort Liability Law to the Civil Code' (2022) 44(3) *European Intellectual Property Review* 162

Quintais JP, 'The New Copyright Directive: A Critique of Article 17' (2020) 42(1) *European Intellectual Property Review* 28

Quintais JP, 'Generative AI and Copyright: A European Perspective' (2025) 16(1) *Journal of Intellectual Property Law & Practice* 12

Quintais JP and Schwemer SF, 'The Interplay between the Digital Services Act and Sector-Specific Intermediary Liability Regimes' (2025) 14(2) *Internet Policy Review* 45

Schwemer SF, 'Trusted Flaggers and the Digital Services Act' (2024) 15(2) *Journal of Intellectual Property, Information Technology and E-Commerce Law* 142

POLICY DOCUMENTS & REGULATORY MATERIALS

Cyberspace Administration of China, *Administrative Measures for Generative Artificial Intelligence Services* (2023, as amended 2025)

European Commission, *Digital Services Act Implementation Guidance and Compliance Materials* (2024–2026 updates)

Ministry of Industry and Information Technology (MIIT), *Unreliable Entities List Enforcement Framework* (2026)

SECONDARY LEGAL CONCEPTS (DOCTRINAL SOURCES)

"Best Efforts Standard" under Directive (EU) 2019/790 Art 17 (CDSM Directive interpretation literature)

"Brussels Effect" (Bradford A, *The Brussels Effect* (2020))

"Cyber Sovereignty" doctrine (Creemers R scholarship)

"Notice and Action Framework" under Regulation (EU) 2022/2065 (DSA)

"Red Flag Test" under Civil Code of the People's Republic of China art 1197

"Notice and Stay-Down Doctrine" (Chinese CSL + judicial interpretation literature)