NOTE

Contractualizing Digital Sovereignty: How China, the UAE, and the United States Embed Censorship and Moderation in Technology Market-Entry Agreements

Chaewon Lee†

States increasingly shape digital platform governance not only through public-law rules, but through contractual and infrastructural arrangements that condition market access and operational control. This Article examines how China, the United Arab Emirates, and the United States embed sovereign authority in platform governance through distinct forms of contractual intervention. In China, licensing restrictions require foreign firms to partner with domestic operators that assume statutory obligations of data localization, identity verification, and content control, embedding censorship within system architecture. In the United Arab Emirates, state control over telecommunications infrastructure enables discretionary, event-triggered intervention, allowing authorities to influence platform behavior through access-based leverage rather than continuous regulation. In the United States, constitutional limits on direct speech regulation channel governmental influence toward national-security mechanisms, particularly CFIUS mitigation agreements, which restructure ownership, data access, and technical control without prescribing moderation outcomes. Across these systems, contract operates as a mechanism for structuring the conditions under which platforms function, rather than as a substitute for public law. The comparative analysis demonstrates that digital sovereignty is increasingly exercised through control over infrastructure, data, and market participation. As a result, governance of digital speech is shifting from direct regulation of content toward the design of the systems that produce, distribute, and control it.

† Cornell University, Class of 2024; J.D. Candidate, Cornell Law School, Class of 2027.

Introduction

States increasingly influence the governance of digital platforms not only through traditional public-law mechanisms, but also through contractual and infrastructural arrangements that condition market access.[1] Telecommunications licensing regimes, cloud-service partnerships, national-security mitigation agreements, and app-distribution terms shape platform conduct in ways that resemble regulatory oversight.[2] As platforms have become central intermediaries for communication, commerce, and political

1. *See infra* Sections I–III.
2. *Id.*

participation, these upstream mechanisms determine who may operate digital infrastructure, how data is managed, and on what terms services reach end users.

This dynamic is especially visible in the domain of content moderation. Scholarly and doctrinal debates have long focused on public-law constraints such as First Amendment limits on compelled speech, intermediary-liability shields like Section 230 of the Communications Act, cybersecurity statutes, and data-protection regimes.[3] In practice, however, platform speech governance also emerges from the contractual conditions of market entry and operation.[4] Access agreements, licensing documents, mitigation covenants, and joint-venture arrangements determine which entities qualify as lawful operators and what obligations accompany participation in digital markets.[5]

The comparative experience of China, the United Arab Emirates, and the United States illustrates distinct configurations of this contractual governance. In China, statutory mandates are operationalized through licensing constraints that require foreign firms to partner with domestic operators capable of executing censorship, data-localization, and access obligations.[6] In the United Arab Emirates, state control over telecommunications infrastructure enables discretionary, event-driven intervention without comprehensive ex ante regulation.[7] In the United States, constitutional constraints—particularly the First Amendment—limit direct speech regulation and instead channel governmental influence through national-security mechanisms that restructure ownership, data custody, and engineering access.[8]

These systems do not converge on a single model of platform governance. Rather, they reflect different ways of embedding sovereign authority into the conditions of technological operation.[9] In China, contract serves as the mechanism through which statutory mandates become

3. John A. LoNigro, *Deplatformed: Social Network Censorship, the First Amendment, and the Argument to Amend Section 230 of the Communications Decency Act*, 37 TOURO L. REV. 427 (2021).

4. *See infra* Sections I–III.

5. *Id.*

6. Telecommunications Regulations of the People's Republic of China (promulgated by the State Council, Sept. 25, 2000, amended Feb. 6, 2016) art. 7 (China); Special Administrative Measures (Negative List) for Foreign Investment Access (2024) (China); Cybersecurity Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017) arts. 12, 28, 37 (China) (hereinafter Cybersecurity Law); Data Security Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., June 10, 2021, effective Sept. 1, 2021) arts. 4–6 (China) (hereinafter Data Security Law); Personal Information Protection Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021) arts. 3, 38–40 (China) (hereinafter Personal Information Protection Law).

7. Federal Decree-Law No. (3) of 2003 Regulating Telecommunications arts. 3, 12, 31, 34 (U.A.E.); Telecommunications & Digital Government Regulatory Authority, Satellite Services Licensing Guide 2–3 (U.A.E.); Telecommunications & Digital Government Regulatory Authority, Licensing Section (U.A.E.).

8. U.S. Const. amend. I; Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), Pub. L. No. 115-232, §§ 1701–28, 132 Stat. 2173.

9. *See infra* Section IV.

operationally enforceable.[10] In the UAE, it functions as a point of leverage through which access may be conditioned or withdrawn.[11] In the United States, it operates as a structural filter that reshapes the architecture of data and control without prescribing substantive moderation outcomes.[12]

Taken together, these developments illustrate how, in certain contexts, digital governance is structured not only through formal legal rules but also through institutional and contractual arrangements that shape control over infrastructure and data. In the jurisdictions examined here, these arrangements help determine which entities may operate platforms, how data is managed, and how regulatory objectives are implemented in practice. In this sense, contract operates as a mechanism through which public authority is operationalized.

I. China's Systemic License-and-Delegate Model

A. Public-Law Foundations and Contractualized Execution

China's digital-governance regime rests on a set of interlocking statutes that impose substantive obligations on network operators and channel those obligations into enforceable structures at the point of market entry. Three statutes form the core of this framework. The Cybersecurity Law requires data localization, real-name registration, and cooperation with public-security authorities, including the provision of technical assistance and access in support of lawful national security and criminal investigations.[13] The Data Security Law builds on this framework by establishing a categorized and graded data protection system, under which data is classified according to its significance to national security and public interests, and by imposing heightened obligations on entities handling "important" and "core" data.[14] The Personal Information Protection Law introduces a formal privacy framework, but one conditioned by state-security priorities: it requires domestic storage for certain categories of data handlers, imposes structured restrictions on cross-border data transfers, and promotes the integration of identity verification and authentication mechanisms within digital services.[15]

Taken together, these statutes impose legally binding obligations of data localization, identity traceability, and state-centered information control.[16] Yet foreign cloud providers cannot directly assume these obligations because they are structurally barred from operating core telecommunications infrastructure in mainland China.[17] The Telecommunications Regulations and implementing rules restrict the licenses required to provide cloud computing,

10. *See infra* Section I.
11. *See infra* Section II.
12. *See infra* Section III.
13. Cybersecurity Law arts. 24, 28, 37, 69.
14. Data Security Law arts. 21, 27, 30.
15. Personal Information Protection Law arts. 10, 38–40, 62(3).
16. Cybersecurity Law arts. 24, 28, 37; Data Security Law arts. 21, 27, 30; Personal Information Protection Law arts. 10, 38–40, 62(3).
17. Telecommunications Regulations arts. 7–9; Provisions on the Administration of Foreign-Invested Telecommunications Enterprises art. 6.

data-center services, and other value-added telecommunications services to PRC-domiciled entities, while imposing strict foreign-ownership caps.[18]

In this model, contract functions as the mechanism through which public-law mandates become operationally enforceable. Licensing rules determine who may qualify as an operator; contractual arrangements determine how that operator is integrated into the platform's technical and organizational architecture. The combination of statutory obligation and licensing constraint ensures that censorship, data localization, and access compliance are embedded upstream, as structural features of system design rather than as downstream responses to discrete enforcement actions.

B. Case Study: Apple iCloud China (GCBD)

1. Migration to a PRC-Licensed Operator

Apple's 2018 reconfiguration of its mainland China iCloud service illustrates how China's regulatory framework translates statutory obligations into enforceable operational arrangements.[19] Beginning in early 2018, Apple notified users that iCloud accounts associated with mainland China would be migrated to infrastructure operated by Guizhou-Cloud Big Data (GCBD), a company owned by the Guizhou provincial government.[20]

This restructuring was not driven by commercial preference alone. Rather, it was compelled by data localization requirements and the broader regulatory framework governing telecommunications services in China. The Cybersecurity Law requires that personal information and important data collected within China be stored domestically, effectively precluding the use of foreign-based cloud infrastructure.[21] At the same time, the Telecommunications Regulations establish a licensing regime for the provision of telecommunications services, including value-added services such as internet-based data processing and storage.[22] These overlapping regulatory requirements required Apple to localize Chinese user data and transfer operational responsibility to a state-linked Chinese partner.

The consequence of this constraint was not merely the need for local data storage, but a restructuring of operational control through a domestically incorporated entity.[23] To offer iCloud services lawfully, Apple was required to partner with a domestic license holder capable of assuming the statutory obligations imposed on network operators.[24] GCBD thus became the entity

---

18. *Id.*

19. *See Apple: Chinese Firm to Operate China iCloud Accounts*, BBC NEWS (Jan. 10, 2018), https://www.bbc.com/news/business-42631386 [https://perma.cc/2PV8-VMFP]; *Apple iCloud: State Firm Hosts User Data in China,* BBC NEWS (July 18, 2018), https://www.bbc.com/news/technology-44870508 [https://perma.cc/SS7F-LFY9].

20. *Id.*

21. Cybersecurity Law art. 37.

22. Telecommunications Regulations arts. 7–8; Ministry of Industry and Information Technology, Classification Catalogue of Telecommunications Services (2015).

23. *Apple iCloud: State Firm Hosts User Data in China*, *supra* note 19.

24. Telecommunications Regulations arts. 7–9; Provisions on Foreign-Invested Telecommunications Enterprises arts. 2, 6.

through which those obligations—data localization, real-name compliance, and government access—would be executed.[25]

2. GCBD as Legal Operator and Contractual Counterparty

The contractual framework governing iCloud China formalizes this allocation of authority. Apple's iCloud terms for mainland China specify that GCBD is the provider of the service and that user data is stored on infrastructure operated by GCBD or its designated partners.[26] Apple's role is defined more narrowly, as providing support and assistance in the provision of the service, rather than serving as the entity responsible for operating it.[27]

This distinction carries significant legal consequences. Under the Cybersecurity Law, Data Security Law, and Personal Information Protection Law, the "network operator" bears responsibility for compliance with data-localization requirements, security reviews, and lawful-access obligations.[28] By structuring iCloud China around GCBD as the operator, Apple positioned a domestic entity—subject to PRC jurisdiction—as the party responsible for fulfilling these duties.

The reallocation of operational authority is reflected in the system's technical configuration. Data associated with Chinese iCloud accounts is stored within China, and this architecture enables government requests to be directed to GCBD, which possesses both the legal obligation and technical capacity to comply.[29] Apple's global model—premised on centralized control over data and encryption—thus gives way to a jurisdiction-specific structure in which control is distributed to a state-affiliated operator.[30]

3. Upstream Enforcement and Architectural Integration

The Apple–GCBD arrangement shifts enforcement from downstream content intervention to upstream system design. Rather than relying on ad hoc takedown requests directed at a foreign provider, the regulatory framework ensures that the entity operating the infrastructure is itself capable of implementing compliance requirements as part of ordinary system operation.[31]

This upstream orientation is also visible in Apple's broader App Store practices in China. Since 2017, roughly 55,000 applications have disappeared from Apple's Chinese App Store, reflecting both compliance with Chinese

25. Cybersecurity Law arts. 24, 28, 37; *Apple iCloud: State Firm Hosts User Data in China*, *supra* note 19.

26. Apple Inc., *iCloud Operated by GCBD Terms and Conditions*, https://www.apple.com/legal/internet-services/icloud/en/gcbd-terms.html [https://perma.cc/P7VY-YZST] (last visited Apr. 16, 2026).

27. *Id.*

28. Cybersecurity Law arts. 24, 28, 37; Data Security Law arts. 21, 27, 30; Personal Information Protection Law arts. 38–40.

29. Cybersecurity Law art. 28; Apple iCloud: State Firm Hosts User Data in China, BBC News.

30. Rafita Ahlam, *Apple, the Government, and You: Security and Privacy Implications of the Global Encryption Debate*, 44 FORDHAM INT'L L.J. 771, 783 (2021).

31. Telecommunications Regulations arts. 7–8; Cybersecurity Law arts. 9, 21, 47.

law and the company's use of internal processes to identify and remove content that may run afoul of regulatory requirements.[32] These practices reflect a compliance environment in which content restrictions are implemented as an ongoing feature of platform governance, rather than triggered solely by discrete government directives.

The iCloud China model therefore illustrates the structural logic of China's license-and-delegate system. Licensing rules determine who may operate; contractual arrangements assign operational responsibility; and statutory obligations define the content and data-governance requirements that must be implemented.[33] The result is a system in which censorship and data access are not external impositions, but features integrated into the architecture of service delivery.

C. Case Study: Microsoft Azure Operated by 21Vianet

1. Regulatory Preconditions and the Necessity of Delegated Operation

Microsoft's cloud operations in mainland China reflect the same licensing constraints that shaped Apple's iCloud restructuring, but they illustrate a distinct dimension of China's regulatory model. As with iCloud, cloud computing services are classified as value-added telecommunications services, subject to foreign-ownership caps and licensing requirements that only PRC-domiciled entities may satisfy.[34] Microsoft therefore cannot operate Azure infrastructure in China as a licensed provider.

To enter the Chinese market, Microsoft structured its operations through a partnership with 21Vianet, a domestic cloud and data-center operator that holds the necessary telecommunications licenses.[35] Under this arrangement, Microsoft supplies software, architecture, and technical support, while 21Vianet assumes the legal status of operator.[36] As a result, the statutory obligations imposed by the Cybersecurity Law, Data Security Law, and Personal Information Protection Law attach to 21Vianet rather than to Microsoft.[37]

This allocation reflects the same license-and-delegate logic observed in Apple's case, but it is more explicitly embedded in an ongoing service model

---

32. Jack Nicas, Raymond Zhong & Daisuke Wakabayashi, *To Get in China, Apple Swallowed Hard Bargain*, N.Y. TIMES (May 18, 2021), https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html [https://perma.cc/YE2J-H54Z].

33. Telecommunications Regulations arts. 7–9; Provisions on Foreign-Invested Telecommunications Enterprises arts. 2, 6; Cybersecurity Law arts. 9–10, 21, 28; Data Security Law arts. 6, 8; Personal Information Protection Law arts. 9, 13.

34. *See* Telecommunications Regulations, *supra* note 17.

35. Microsoft, *Azure in China Checklist*, https://learn.microsoft.com/en-us/azure/china/overview-operations [https://perma.cc/W97T-KD45] (last visited Apr. 12, 2026); Microsoft, Microsoft Azure Operated by 21Vianet, https://learn.microsoft.com/en-us/azure/china/overview-checklist [https://perma.cc/Q5DC-8U29]; Marcos Sabio, *The Complete Guide to Microsoft Azure China*, APPINCHINA Dec. 18, 2025), https://appinchina.co/a-guide-to-microsoft-azure-in-china/ [https://perma.cc/4P5G-WYKY].

36. *Id.*

37. *Id.*

rather than a one-time migration. Microsoft does not act as the licensed telecommunications operator and instead provides technology and services through a locally licensed partner, which assumes primary regulatory compliance obligations under Chinese law.[38]

2. Contractual Architecture and Operator Responsibility

The contractual framework governing Azure China reinforces this allocation of authority. Customers contract with 21Vianet, not Microsoft, for the provision of cloud services within mainland China.[39] Service agreements designate 21Vianet as the provider responsible for data storage, compliance, and customer relationships, while Microsoft remains a technology supplier supporting the underlying platform.[40]

Microsoft itself distinguishes Azure China from its global cloud by describing it as a "physically separated" instance operated independently by 21Vianet.[41] This separation is not merely technical; it reflects a legal and regulatory boundary. Data generated by customers in China is processed and stored within infrastructure controlled by 21Vianet, and access is governed by PRC law.[42]

Operational practices further reflect this structure. Real-name authentication, required under Chinese law, is implemented by 21Vianet, which collects and verifies identifying information from users.[43] Customer data is processed within China on infrastructure operated by a domestic provider, and is governed by Chinese legal and regulatory requirements, including obligations relating to content control and cooperation with authorities.[44] Microsoft's access to such data is limited and mediated through its relationship with the domestic operator.[45]

Together, these arrangements ensure that the entity with legal responsibility for compliance also possesses the technical capacity to fulfill it. Contract aligns statutory obligation with operational control, placing both within the jurisdiction of the PRC.

3. Lifecycle Governance and Market Implications

The Azure–21Vianet arrangement illustrates how China's regulatory model extends beyond initial market entry to shape the ongoing evolution of platform services. Because 21Vianet controls infrastructure and bears legal responsibility for compliance, it serves as the interface through which

38. *Id.*

39. Microsoft, *supra* note 35; 21Vianet, *Online Services Terms* (Oct. 1, 2025), https://en.21vbluecloud.com/ostpt [https://perma.cc/X33W-JJB9].

40. *Id.*

41. Microsoft, *supra* note 35.

42. Sabio, *supra* note 35.

43. Microsoft, Data Sovereignty and China Regulations, https://learn.microsoft.com/en-us/azure/china/overview-sovereignty-and-regulations [https://perma.cc/VH5U-WKH7] (last visited Apr. 12, 2026).

44. Microsoft, *supra* note 35; 21Vianet, *supra* note 39.

45. Microsoft, *supra* note 35; Sabio, *supra* note 35.

regulatory requirements are continuously implemented.[46]

This structure has implications for both governance and competition. Customers using Azure China operate within a system in which data access, storage, and processing are subject to PRC law, including potential government access under lawful process.[47] At the same time, Microsoft faces competitive pressure from domestic cloud providers whose services are natively aligned with the regulatory environment and do not require the same degree of structural separation.[48]

The 21Vianet model thus reveals a broader feature of China's license-and-delegate system. Contract does not merely enable foreign entry; it defines the terms under which foreign technology is domesticated. Through licensing constraints and contractual allocation, foreign cloud services are transformed into infrastructure that is locally operated, jurisdictionally bounded, and continuously subject to regulatory oversight.

II. UAE's Selective Permit-and-Filter Model

A. Regulatory Environment and Enforcement Discretion

The United Arab Emirates employs a more fragmented and discretionary approach to digital platform governance than the integrated statutory regime found in China. Rather than imposing comprehensive, system-wide obligations on platforms, the UAE relies on overlapping criminal prohibitions, media-regulation standards, and telecommunications controls to manage online content.

Federal Decree-Law No. 34 of 2021 on Countering Rumors and Cybercrimes establishes multiple categories of prohibited expression, including content that threatens public order, public morals, national unity, or the reputation of the State.[49] These categories are defined at a high level of generality and do not prescribe specific technical or operational requirements for platforms.[50] Instead, they establish broad substantive standards that authorize enforcement actions—including removal and access-blocking orders—when content falls within prohibited categories.[51]

This framework is reinforced by the UAE's media-regulation regime. Authority over media content is exercised by federal institutions, including the UAE Media Council, which oversees compliance with standards prohibiting content that insults religion, undermines national unity, or

46. *See* Microsoft, *supra* note 35; Sabio, *supra* note 35; Telecommunications Regulations arts. 7–9; Provisions on Foreign-Invested Telecommunications Enterprises arts. 2, 6; Cybersecurity Law arts. 9–10, 21, 28; Data Security Law arts. 6, 8; Personal Information Protection Law arts. 9, 13.

47. Cybersecurity Law, arts. 21, 37; Data Security Law arts. 21, 31; Personal Information Protection Law arts. 38–40.

48. Julien Dylan Isaacs, *Digital Expansionism: Exploring the U.S.–China Technology Dynamic Through Cybersecurity Policy and International Marketing Strategies in the Cloud Computing Sector* 50–52 (2019) (M.S. thesis, Mass. Inst. Tech.).

49. Federal Decree-Law No. 34 of 2021 arts. 22–25, 34 (U.A.E.).

50. *Id.*

51. *Id.* arts. 22–25, 62.

violates public morals.[52] As with the cybercrime framework, these standards do not prescribe specific platform-level technical requirements.[53] Instead, they establish substantive prohibitions that are enforced through oversight, inspection, and administrative sanctions.[54]

The principal mechanism of enforcement, however, lies in the telecommunications layer. The Telecommunications and Digital Government Regulatory Authority (TDRA) implements the Internet Access Management (IAM) Policy, which requires licensed internet service providers to block access to categories of prohibited content using technical filtering systems integrated with their networks.[55] Enforcement is thus directed primarily at distribution infrastructure rather than at platforms themselves.

This design is made possible by the structure of the UAE's telecommunications market. Public telecommunications services are provided primarily by two state-linked carriers—e& and du—which together dominate internet access infrastructure.[56] As a result, these operators function as key intermediaries through which digital services reach end users.[57] Although foreign platforms may offer services directly to users, they remain dependent on locally licensed carriers for network access, enabling the State to retain a persistent point of control over distribution.[58]

Taken together, these elements produce a model of governance centered on discretionary enforcement rather than continuous regulation. Legal standards define broad categories of prohibited content, leaving substantial discretion in how and when enforcement is pursued.[59] Control over telecommunications infrastructure ensures that, when intervention occurs, it can be implemented effectively through network-level measures, without requiring detailed, platform-specific mandates.[60]

Moderation in the UAE is therefore not embedded in platform architecture as a standing obligation. It operates as a contingent capability,

---

52. Federal Decree-Law No. 55 of 2023 arts. 17, 22 (U.A.E.).

53. *Id.*

54. *Id.* arts. 22–23.

55. Telecommunications & Digital Government Regulatory Authority, Internet Access Management Regulatory Policy §§ 3–4 (Apr. 19, 2017).

56. Dan Murphy, *UAE Telco e&, Formerly Etisalat, Sets Sights on Asia, Europe for Growth After Major Overhaul*, CNBC (Mar. 3, 2022), https://www.cnbc.com/2022/03/03/uae-telco-e-formerly-etisalat-aims-for-asia-europe-growth-after-overhaul.html [https://perma.cc/GQ2V-7VEK]; Telecommunications Regulatory Authority, Regulatory Policy: Voice over Internet Protocol § 3.1 (Dec. 30, 2009).

57. Telecommunications & Digital Government Regulatory Authority, Internet Access Management Regulatory Policy, *supra* note 55.

58. *Id.*

59. Federal Decree-Law No. 34 of 2021 arts. 23–25, 34 (U.A.E.); Telecommunications & Digital Government Regulatory Authority, Internet Access Management Regulatory Policy, *supra* note 55; Telecommunications & Digital Government Regulatory Authority, Prohibited Content Categories, https://tdra.gov.ae/en/about/tdra-sectors/information-and-digital-government/policy-and-programs-department/internet-guidelines#prohibited-content-categories [https://perma.cc/X6KN-85VG].

60. *Id.*

exercised through control of access and distribution rather than through continuous technical filtering.

B. Contractual Intermediation: Telecom Gatekeeping and Platform Dependence

Foreign technology firms cannot operate telecommunications infrastructure or provide telecommunications services in the United Arab Emirates without obtaining a license from the TDRA or operating through arrangements with licensed domestic providers.[61] In practice, telecommunications licenses are held by an effective duopoly of state-linked carriers—e& and du—that dominate internet access infrastructure.[62] As a result, foreign platforms remain dependent on these carriers' networks to reach users within the UAE.[63]

Unlike systems that impose detailed ex ante moderation obligations, the UAE regulatory framework centers on the ability to control access through licensed telecommunications providers.[64] Regulatory policies require licensees to implement mechanisms to block or permit access to internet content, while the broader telecommunications regime ensures that network operators remain subject to ongoing regulatory supervision.[65] This structure allows authorities to restrict or disable access to services through licensed intermediaries, ensuring that intervention can be implemented through the ordinary operation of telecommunications infrastructure.[66]

Cloud-service arrangements reflect the same structural logic. Providers such as Amazon Web Services and Microsoft Azure operate regional infrastructure within the UAE that emphasizes data residency and compliance with domestic data-protection requirements.[67] These configurations align cloud services with local regulatory frameworks and enable organizations to meet applicable legal and compliance obligations through infrastructure located within the jurisdiction.[68] The contractual and infrastructural

---

61. Murphy, *supra* note 56; Telecommunications Regulatory Authority, Regulatory Policy: Voice over Internet Protocol, *supra* note 56.

62. *Id.*

63. Telecommunications & Digital Government Regulatory Authority, Internet Access Management Regulatory Policy, *supra* note 55.

64. Federal Decree-Law No. (3) of 2003 Regulating Telecommunications arts. 3, 12 (U.A.E.).

65. Telecommunications and Digital Government Regulatory Authority, Internet Access Management Regulatory, supra note 55; Federal Decree-Law No. (3) of 2003 arts. 12–14 (U.A.E.).

66. Federal Decree-Law No. (34) of 2021 art. 38; Telecommunications & Digital Government Regulatory Authority, Internet Access Management Regulatory Policy, supra note 55.

67. Microsoft, *Microsoft Cloud Datacenter Regions Now Available in the UAE to Help Fuel the Middle East's Future Economic Ambitions* (June 19, 2019), https://news.microsoft.com/en-xm/2019/06/19/microsoft-cloud-datacenter-regions-now-available-in-the-uae-to-help-fuel-the-middle-easts-future-economic-ambitions/ [https://perma.cc/542Y-7FPZ]; Amazon Web Services, *United Arab Emirates Data Privacy*, https://aws.amazon.com/compliance/uae_data_privacy/ [https://perma.cc/R5VH-QBVW](last visited Apr. 16, 2026).

68. *Id.*

framework thus embeds the capacity for compliance without prescribing continuous content control.

The dynamics of this system are evident in instances of platform adjustment following regulatory pressure. In 2022, Amazon restricted LGBTQ-related search results in the UAE after receiving government concerns, despite the absence of a publicly issued legal mandate requiring such filtering.[69] The episode illustrates how enforcement operates through relational leverage rather than formal command: platforms that depend on state-controlled infrastructure anticipate that continued access may hinge on responsiveness to regulatory signals.

A similar pattern appears in the regulation of Voice-over-IP (VoIP) services. VoIP functionality in widely used communication applications is selectively restricted through network-level filtering implemented by local internet service providers.[70] As a result, global platforms have experienced blocking or disruption of VoIP calling features within the UAE, even while other functionalities remain available.[71] These practices illustrate how control over telecommunications infrastructure enables the selective limitation of service functionality without requiring platform-specific design mandates.

Together, these arrangements show that the UAE's governance model does not embed censorship directly in platform architecture. Instead, it relies on contractual intermediation to maintain a flexible form of control. Platforms operate within a system in which intervention is not constant but remains readily available, exercised through infrastructure when circumstances demand.

C. Case Studies: Netflix and TikTok

Recent episodes involving Netflix and TikTok illustrate how the UAE's governance model operates through selective, event-triggered intervention rather than continuous regulatory control.[72] These examples highlight two

---

69. Julia Kollewe, *Amazon Bows to UAE Pressure to Restrict LGBTQ+ Search Results*, GUARDIAN (June 30, 2022), https://www.theguardian.com/technology/2022/jun/30/amazon-bows-to-uae-pressure-to-restrict-lgbt-search-results [https://perma.cc/93EJ-58T7]; Natasha Turak, *Amazon Blocks Searches for LGBTQ+ Products in the United Arab Emirates*, CNBC (July 1, 2022), https://www.cnbc.com/2022/07/01/amazon-blocks-searches-for-lgbtq-products-in-the-united-arab-emirates.html [https://perma.cc/2EQS-UPYP].

70. Telecommunications Regulatory Authority, Regulatory Policy: Voice over Internet Protocol § 3.1 (Dec. 30, 2009) (U.A.E.); Friedemann Lipphardt et al., Can You Hear Me? A First Study of VoIP Censorship Techniques in Saudi Arabia and the UAE, IEEE EUR. SYMP. ON SEC. & PRIV. 720, 720–23 (2025).

71. *Id.*

72. Guardian, *Six Gulf States Warn Netflix Over Content Violating "Islamic Values"* (Sept. 6, 2022), https://www.theguardian.com/world/2022/sep/07/six-gulf-states-warn-netflix-over-content-violating-islamic-values [https://perma.cc/GX2C-UE5J]; David Gritten, *Netflix: Saudi Arabia and GCC Warn Streaming Giant Over Violating 'Islamic Values,'* BBC NEWS (Sept. 6, 2022), https://www.bbc.com/news/world-middle-east-62811522 [https://perma.cc/YU7D-874L]; Abbas Al Lawati et al., *Gulf Arab States Demand Netflix Remove 'Immoral Content,'* CNN (Sept. 7, 2022), https://www.cnn.com/2022/09/07/media/netflix-gulf-warning-mime-intl [https://perma.cc/W4QP-7TBN]; Times of India, *UAE: TikTok Removes Over 1 Million Videos in Q1 2025 for Policy Violations* (Aug. 5, 2025),

defining features of the system: the use of coordinated signaling to pressure platforms and the role of infrastructural dependence in securing compliance.

1. *Netflix and the Activation of Cultural Enforcement*

In 2022, the UAE joined other Gulf Cooperation Council (GCC) states in issuing a public warning to Netflix regarding content deemed inconsistent with "Islamic and societal values," including material accessible to children.[73] Although the statement did not identify specific titles in formal regulatory terms, state-affiliated media highlighted programming that included LGBTQ representation and framed it as incompatible with regional norms.[74]

The significance of this episode lies less in the substance of the content than in the mechanism of enforcement. No publicly issued legal directive required Netflix to implement categorical filtering across its platform. Instead, the State signaled that continued distribution was contingent on responsiveness to these concerns.[75] Given the platform's reliance on domestic telecommunications infrastructure, such signaling carried credible weight: access could be restricted or degraded if expectations were not met.

This form of intervention reflects a model in which enforcement is activated by salience rather than embedded as a standing technical requirement. When particular content categories become politically or culturally charged, the State can induce compliance without articulating detailed ex ante rules.

2. *TikTok and Anticipatory Compliance*

TikTok's moderation practices in the UAE illustrate a complementary dynamic: platforms often adjust behavior in anticipation of potential intervention. Public reporting indicates that TikTok removes substantial volumes of content in the UAE, with high rates of proactive enforcement and rapid takedown timelines.[76]

These patterns are consistent with a regulatory environment in which the boundaries of permissible content are broadly defined and enforcement is discretionary.[77] Because TikTok operates within infrastructure controlled by state-affiliated carriers, the cost of non-compliance—whether in the form of access restrictions or regulatory scrutiny—creates incentives for

---

https://timesofindia.indiatimes.com/world/middle-east/uae-tiktok-removes-over-1-million-videos-in-q1-2025-for-policy-violations/articleshow/123110919.cms [https://perma.cc/NHP2-H4VB]; Khaleej Times, *UAE: TikTok Removes Over 1 Million Videos in 3 Months for Violating Guidelines* (Aug. 4, 2025), https://www.khaleejtimes.com/uae/tiktok-removes-over-1-million-videos-community-guidelines [https://perma.cc/J5AV-9S32].

73. Guardian, *supra* note 72; Gritten, *supra* note 72; Lawati et al., *supra* note 72.

74. *Id.*

75. *Id.*

76. Times of India, *supra* note 72; Khaleej Times, *supra* note 72.

77. Federal Decree-Law No. 34 of 2021 arts. 1, 38 (U.A.E.); Federal Decree-Law No. 55 of 2023 arts. 5–6 (U.A.E.); Telecommunications & Digital Government Regulatory Authority, Internet Access Management Regulatory Policy § 3-1; Federal Decree-Law No. 3 of 2003 arts. 3, 12–14 (U.A.E.).

precautionary moderation.[78]

This anticipatory posture does not result from detailed statutory mandates directing platform behavior. Rather, it reflects the platform's effort to align with perceived regulatory expectations in a system where intervention is possible but not continuously exercised.

3. Implications for Episodic Governance

Taken together, these cases illustrate how the UAE's model operates along two temporal dimensions. In the Netflix episode, enforcement follows a triggering event, with regulatory pressure applied after content becomes salient.[79] In the TikTok context, enforcement is preemptive, as platforms adjust behavior to avoid triggering intervention in the first place.[80]

Both dynamics depend on the same underlying structure: control over distribution infrastructure. Because platforms must reach users through licensed telecommunications providers, the State retains the capacity to intervene at the network level by directing those providers to restrict or disable access pursuant to applicable legal authorities.[81]

D. Enforcement as Relational Leverage

The UAE's approach to platform governance is shaped not only by its enforcement practices but also by its broader economic strategy.[82] The State simultaneously seeks to position itself as a regional digital and innovation hub while retaining the capacity to regulate cross-border communications.[83] This dual objective produces a system in which openness and control coexist, mediated through infrastructure rather than formal rulemaking.

This dynamic is particularly visible in the regulation of communication services. Historically, VoIP platforms have been restricted unless routed through licensed domestic carriers, ensuring that communications remain within infrastructure subject to state oversight.[84] During the COVID-19 pandemic, however, the government temporarily relaxed certain restrictions, permitting the use of selected enterprise communication tools to support remote work and economic continuity.[85] These measures did not represent a structural shift toward liberalization.[86] Instead, they demonstrated the State's ability to recalibrate access conditions in response to changing circumstances

78. *Id.*

79. Guardian, *supra* note 72; Gritten, *supra* note 72; Lawati et al., *supra* note 72.

80. Times of India, *supra* note 72; Khaleej Times, *supra* note 72.

81. Federal Decree-Law No. 3 of 2003 arts. 3, 12–14 (U.A.E.); Federal Decree-Law No. 34 of 2021 art. 38 (U.A.E.).

82. *UAE Digital Economy Strategy Fuels Tech Transformation,* REUTERS (Oct. 25, 2024).

83. *Id.*

84. Natasha Turak, *UAE Loosens Some VoIP Restrictions as Residents in Lockdown Call for End to WhatsApp and Skype Ban*, CNBC (Mar. 26, 2020), https://www.cnbc.com/2020/03/26/coronavirus-lockdown-uae-residents-call-for-end-to-whatsapp-skype-ban.html [https://perma.cc/5ALZ-V3CB].

85. *Id.*

86. *Id.*

while preserving underlying control over distribution channels.[87]

This pattern reflects a broader feature of the UAE's governance model: regulatory flexibility grounded in infrastructural control. The State does not rely on continuous, system-wide mandates to shape platform behavior but rather maintains a capacity to adjust the scope of permissible activity, expanding or contracting access as economic, political, or social conditions evolve.[88]

In this sense, enforcement in the UAE operates as relational leverage rather than as systemic engineering. The State does not attempt to redesign platform architecture or impose continuous filtering obligations. Instead, it conditions participation in the domestic market on an ongoing relationship in which compliance can be demanded when circumstances warrant.

This model differs from both China's anticipatory system and the United States' structural, risk-based approach.[89] It is neither continuously embedded in infrastructure nor entirely detached from content considerations.[90] Rather, it occupies an intermediate position: a system of reserve authority, in which the capacity to intervene shapes platform behavior even when intervention is not actively exercised.

The result is a governance architecture defined by elasticity. Platforms are permitted to operate, but the boundaries of permissible activity remain adjustable. Control is not expressed through constant enforcement, but through the credible possibility of intervention, enabled by the State's position at the level of distribution infrastructure.

III. United States' Screen-and-Mitigate Model

A. Constitutional and Statutory Constraints

The United States approaches digital platform governance within a constitutional framework that sharply limits the government's ability to impose direct content-moderation mandates. Under the First Amendment, private platforms are treated as entities with editorial discretion over the content they host, rank, or remove.[91] As a result, the government generally cannot compel platforms to alter or distribute speech based on viewpoint.[92] Efforts to impose such obligations—whether through state legislation or regulatory initiatives—encounter constitutional limits grounded in the protection of editorial judgment.[93]

Federal statutory law reinforces this structure without displacing it. Section 230 of the Communications Act provides immunity for platforms with respect to third-party content while preserving their discretion to remove

87. *Id.*
88. *Id.*
89. *See supra* Section I; *infra* Section III.
90. *Id.*
91. U.S. Const. amend. I; Ashutosh Bhagwat, *Do Platforms Have Editorial Rights?*, 1 J. FREE SPEECH L. 97 (2021).
92. *See, e.g.,* Miami Herald Publ'g Co. v. Tornillo, 418 U.S. 241, 258 (1974).
93. *Id.*

material in good faith.[94] Rather than establishing substantive moderation requirements, Section 230 protects private ordering by shielding platforms from liability and allowing them to determine their own content policies.[95]

These constraints do not eliminate federal influence over platform governance, but they channel it away from direct speech regulation. Within this framework, the Committee on Foreign Investment in the United States (CFIUS) has emerged as a central mechanism of regulatory influence.[96] Through its authority to review and condition foreign investments, CFIUS imposes mitigation agreements that restructure ownership, data access, and technical control.[97] These agreements do not regulate content directly.[98] Instead, they shape the institutional and infrastructural conditions under which content moderation occurs.[99]

The result is a model of governance defined by structural intervention rather than expressive regulation. The federal government does not prescribe what platforms must remove or promote; it determines who may control the systems through which information is stored, processed, and distributed.

B. Contractual Security Mitigation as Moderation-by-Proxy

The principal mechanism through which the United States influences platform governance is not direct regulation of speech, but contractual national-security mitigation. Through CFIUS, the federal government negotiates agreements that condition market access on structural changes to ownership, data governance, and technical control.[100] These agreements rarely address content moderation explicitly but rather regulate the underlying systems that make moderation possible.[101]

CFIUS-related national security frameworks and adjacent regulatory regimes addressing foreign access to U.S. data impose requirements concerning data access restrictions, security controls, audit mechanisms, and oversight of transactions involving sensitive personal data.[102] These measures include limiting or prohibiting foreign access to bulk U.S. sensitive personal data, conditioning certain transactions on compliance with predefined

94. 47 U.S.C. § 230.

95. *Id.*

96. 50 U.S.C. § 4565; Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), Pub. L. No. 115-232, §§ 1701–1728, 132 Stat. 2173; U.S. Dep't of the Treasury, *CFIUS Mitigation*, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-mitigation [https://perma.cc/JE2R-HF5X] (last visited Apr. 12, 2026).

97. 50 U.S.C. § 4565.

98. Anupam Chander & Paul Schwartz, *The President's Authority Over Cross-Border Data Flows*, 172 U. PA. L. REV. 1989 (2023).

99. *Id.*

100. 50 U.S.C. § 4565; FIRRMA, *supra* note 96; U.S. Dep't of the Treasury, *supra* note 96.

101. *Id.*

102. Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 1636, 1637–38 (Jan. 8, 2025); Harry Clark et al., *U.S. Data Localization Law Coming Soon*, ORRICK (Jan. 17, 2025), https://www.orrick.com/en/Insights/2025/01/US-Data-Localization-Law-Coming-Soon-DOJ-Issues-Final-Rule [https://perma.cc/98YL-S92P].

security requirements, and structuring vendor, employment, and investment relationships to mitigate risks associated with foreign access.[103] In addition, regulatory frameworks require ongoing compliance mechanisms such as due diligence, reporting, and audit-related obligations designed to monitor and enforce adherence to these restrictions.[104] These obligations operate through legally binding conditions on transactions and agreements, with violations subject to civil and criminal penalties, reflecting an enforcement model grounded in conditional authorization and ongoing compliance rather than direct ex ante prohibition of all transactions.[105]

Although these measures do not prescribe specific moderation outcomes, they reshape the structural and technical conditions under which content is organized and made visible. Moderation operates through governance mechanisms that influence what content is surfaced, prioritized, and disseminated, often by structuring the flow of content within a platform's underlying systems.[106] Changes to data access, system design, and oversight can therefore alter how content is ranked and managed, even without directly dictating substantive moderation decisions.[107]

In this way, mitigation agreements operate as a form of moderation-by-proxy. By altering control over data, code, and infrastructure, the government indirectly shapes the conditions under which platforms exercise editorial discretion. The regulatory focus is not on speech itself, but on the architecture that produces and organizes it.

C. Sovereignty Through Risk Screening, Not Content Control

The United States often exercises digital sovereignty through risk-based intervention rather than direct content-based regulation. In this context, federal action is triggered not by the presence of particular speech, but by concerns about ownership, data access, and the potential for foreign influence over platform infrastructure.[108] This design reflects constitutional constraints: the government cannot prescribe moderation outcomes, but it may regulate the structural conditions that give rise to them.[109]

Within this framework, national-security risk functions as the organizing principle of platform governance. The relevant questions are not what content a platform hosts, but who controls its data, who can access its systems, and who can influence its technical operations.[110] When these factors raise concerns about foreign leverage—particularly in relation to sensitive personal data or algorithmic control—regulatory intervention becomes possible.[111]

---

103. *Id.*
104. *Id.*
105. *Id.*
106. James Grimmelmann, *The Virtues of Moderation*, 17 YALE J.L. & TECH. 42, 45–47 (2015).
107. *Id.* at 55–56; *see also* 90 Fed. Reg. 1636, *supra* note 102.
108. 90 Fed. Reg. 1636, *supra* note 102, at 1637–38.
109. U.S. Const. amend. I; 47 U.S.C. § 230; Preventing Access to U.S. Sensitive Personal Data, supra note 102.
110. 90 Fed. Reg. 1636, *supra* note 102.
111. *Id.*

CFIUS mitigation agreements operationalize this approach by targeting the inputs that shape platform behavior. Restrictions on data access, limits on foreign control over corporate governance and operations, and structural separation between U.S. and foreign entities are designed to reduce the risk that foreign actors could exploit sensitive personal data or digital infrastructure for strategic purposes.[112] These measures do not typically prescribe specific content outcomes.[113] Instead, they operate at the level of ownership, access, and control, thereby structuring the conditions under which platform governance occurs.[114]

This risk-screening model differs fundamentally from systems that regulate speech directly or that rely on discretionary intervention in response to specific content. Unlike China's approach, which embeds censorship obligations into the identity of the operator, the United States does not impose continuous moderation requirements.[115] And unlike the UAE's model, which enables episodic intervention when content becomes salient, the United States focuses on structural vulnerabilities that exist independently of any particular piece of speech.[116]

Moderation in this system is therefore a derivative effect of structural regulation. By determining who may control data, infrastructure, and code, the federal government shapes the environment in which platforms exercise editorial discretion without dictating the outcomes of that discretion. Governance operates through the configuration of systems rather than through commands directed at speech itself.

D. CFIUS and the Rise of National-Security-Driven Data Governance

CFIUS's recent interventions reflect a shift in U.S. national-security doctrine from traditional concerns with defense and critical infrastructure to a broader focus on data governance and platform control. Historically, foreign-investment review centered on sectors involving military capability, energy systems, or dual-use technologies.[117] Over the past decade, however, federal authorities have increasingly treated large-scale personal data as a strategic asset whose control may implicate national security.[118]

Congress formalized this shift through the Foreign Investment Risk Review Modernization Act (FIRRMA), which expanded CFIUS's jurisdiction to include transactions involving sensitive personal data of U.S. persons.[119] Under this framework, the national-security analysis turns on whether foreign ownership could enable access to datasets capable of revealing behavioral patterns, personal vulnerabilities, or network

112. *Id.*
113. *Id.*
114. *Id.*
115. *See supra* Section I.
116. *See supra* Section II.
117. Heath P. Tarbert, Modernizing CFIUS, 88 GEO. WASH. L. REV. 1477, 1483, 1485–86 (2020).
118. Preventing Access to U.S. Sensitive Personal Data, supra note 102; FIRRMA, supra note 96.
119. FIRRMA, supra note 96.

relationships.[120]

The Grindr and PatientsLikeMe cases illustrate how this expanded conception of risk operates in practice.[121] Both platforms collected highly sensitive user data—ranging from geolocation and personal communications to health information—and both were acquired by Chinese firms without initial CFIUS review.[122] In each case, the federal government later intervened and required divestiture.[123]

In the Grindr transaction, officials concluded that foreign ownership created unacceptable risks because the platform aggregated location data, private messages, and information about users' sexual orientation.[124] These datasets could be used to identify individuals with security clearances, map their movements, and potentially subject them to coercion or blackmail.[125] The concern was not tied to any specific content hosted on the platform, but to the structural possibility that sensitive data could be accessed or exploited by a foreign government.[126]

The PatientsLikeMe intervention followed a similar logic. The platform enabled users to share detailed health information, including diagnoses, treatment histories, and disease progression.[127] When a Chinese firm acquired a majority stake, CFIUS determined that access to this data—particularly when combined with other datasets—posed national-security risks.[128] As in Grindr, the issue was not how the platform moderated user content, but who controlled the data infrastructure underlying that content.

These cases demonstrate that the United States increasingly regulates platforms by targeting ownership structures that enable data access, rather than by regulating platform behavior directly. Contractual or quasi-contractual interventions—whether through mitigation agreements or forced divestitures—serve to reassign control over data and infrastructure to entities deemed compatible with national-security interests.

In this model, data is treated not simply as an economic resource but as a vector of strategic vulnerability. Regulatory action is triggered when control over that data raises concerns about foreign influence, regardless of whether the platform's visible content practices are themselves problematic.

---

120. *Id.*

121. Georgia Wells & Kate O'Keeffe, U.S. Orders Chinese Firm to Sell Grindr, WALL ST. J. (Mar. 27, 2019), https://www.wsj.com/articles/u-s-orders-chinese-company-to-sell-grindr-app-11553717942 [https://perma.cc/NH82-PEF5]; Harry Clark et al., *Grindr and Patients Like Me Outcomes*, ORRICK (Apr. 23, 2019), https://www.orrick.com/en/Insights/2019/04/Grindr-and-PatientsLikeMe-Outcomes-Show-Non-Cleared-Transactions-Exposure-to-CFIUS-Scrutiny [https://perma.cc/2RMH-A6KA]; Reuters, *U.S. Pushes Chinese Owner of Grindr to Divest*, VENTUREBEAT (Mar. 27, 2019), https://venturebeat.com/ai/u-s-pushes-chinese-owner-of-grindr-to-divest-the-dating-app [https://perma.cc/UL3F-79GY].

122. *Id.*

123. *Id.*

124. Wells & O'Keeffe, *supra* note 121; Clark et al., *supra* note 121.

125. *Id.*

126. *Id.*

127. Farr & Levy, *supra* note 121.

128. *Id.*

E. Case Study: TikTok and the Consolidation of Structural Governance

TikTok represents the most visible example of the United States' shift toward structural, national-security-based governance of digital platforms. Federal concern has centered not on the content disseminated through the platform, but on the relationship between TikTok's U.S. operations and its parent company, ByteDance, and the resulting risks associated with data access and algorithmic control.[129]

Through CFIUS review, the federal government sought to address these concerns by restructuring the conditions under which TikTok operates in the United States.[130] Proposed mitigation measures included requirements that U.S. user data be stored domestically, that access to that data be restricted to U.S.-based personnel, and that sensitive components of the platform—such as recommendation systems—be subject to oversight by approved auditors.[131]

When negotiations over mitigation stalled, Congress enacted legislation conditioning TikTok's continued operation on divestiture from its foreign parent.[132] In *TikTok Inc. v. Garland*, the Supreme Court treated this intervention as implicating the First Amendment but upheld it on the ground that it addressed national-security risks associated with ownership and control rather than regulating speech directly.[133] The remedy—structural reorganization—was thus understood as distinct from censorship.

The TikTok episode illustrates the consolidation of a governance model in which the State intervenes by reshaping the architecture of platform control. Rather than directing what content may appear on the platform, the federal government seeks to determine who may access user data, who may influence algorithmic systems, and how corporate governance structures insulate domestic operations from foreign authority.

In this framework, algorithmic control becomes a focal point of regulatory concern. Recommendation systems determine how content is ranked, amplified, and personalized, and therefore play a central role in shaping the information environment.[134] By restricting access to these systems or requiring oversight mechanisms, the government indirectly influences the conditions under which content is distributed without prescribing substantive moderation rules.

TikTok thus exemplifies the defining feature of the U.S. approach: governance through structural intervention rather than expressive regulation. The State does not attempt to align platform content with regulatory preferences. Instead, it defines a permissible configuration of ownership, data governance, and technical control, within which platforms retain formal editorial autonomy.

---

129. TikTok Inc. v. Garland, 122 F.4th 941, 941–42, 944 (D.C. Cir. 2024).

130. Exec. Order No. 14,350, 90 Fed. Reg. 60,001, § 2(b)–(c) (Sept. 25, 2025).

131. *Id.*

132. Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H, §§ 2–3, 138 Stat. 895 (2024).

133. TikTok Inc. v. Garland, 145 S. Ct. 57 (2025).

134. Pau Muñoz et al., *The Role of Recommendation Algorithms in the Formation of Disinformation Networks*, 62 INFO. PROCESSING & MGMT. 1–3 (2025).

IV. Comparative Analysis: Three Models of Contractual Digital Sovereignty

A. Structural Comparison

Across China, the United Arab Emirates, and the United States, digital sovereignty is implemented not only through public-law directives but through contractual arrangements that determine who may operate within national digital environments and on what conditions. In each system, contract functions as a mechanism for translating sovereign objectives into operational control. What differs is where authority is embedded and how it is exercised.

China locates authority at the level of the operator.[135] Because foreign firms cannot obtain the licenses required to provide cloud or telecommunications services, they must partner with domestic entities that assume legal responsibility for compliance.[136] Statutory obligations—data localization, identity verification, and content control—attach to these operators and are implemented as continuous features of system design.[137] Contract operates as the mechanism through which those obligations are assigned to entities capable of executing them.[138]

The UAE locates authority at the level of access.[139] Platforms may operate without continuous, system-wide obligations, but they remain dependent on state-controlled telecommunications infrastructure.[140] This dependence enables intervention when particular content becomes politically or culturally salient.[141] Contractual relationships with domestic carriers provide the leverage through which compliance can be induced, even in the absence of detailed ex ante regulation.[142]

The United States locates authority at the level of control over infrastructure.[143] Constitutional constraints preclude direct regulation of platform speech, but the government may structure ownership, data access,

---

135. Cybersecurity Law arts. 24, 28, 37; Data Security Law arts. 21, 27, 30; Personal Information Protection Law arts. 38–40.

136. Telecommunications Regulations arts. 7–9; Provisions on Foreign-Invested Telecommunications Enterprises art. 6 (China).

137. Cybersecurity Law arts. 24, 28, 37; Data Security Law arts. 21, 27, 30; Personal Information Protection Law arts. 10, 38–40.

138. Telecommunications Regulations arts. 7–9; Provisions on Foreign-Invested Telecommunications Enterprises arts. 2, 6; Cybersecurity Law arts. 9–10, 21, 28.

139. Telecommunications & Digital Government Regulatory Authority, Internet Access Management Regulatory Policy, *supra* note 55; Federal Decree-Law No. 34 of 2021 arts. 22–25 (U.A.E.).

140. Federal Decree-Law No. 3 of 2003 arts. 3, 12 (U.A.E.); Telecommunications & Digital Government Regulatory Authority, Internet Access Management Regulatory Policy, *supra* note 55.

141. Federal Decree-Law No. 34 of 2021 arts. 23–25, 34, 38 (U.A.E.).

142. Federal Decree-Law No. 3 of 2003 arts. 12–14 (U.A.E.); Telecommunications & Digital Government Regulatory Authority, Internet Access Management Regulatory Policy, *supra* note 55.

143. 50 U.S.C. § 4565; Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 1636, 1637–38 (Jan. 8, 2025).

and technical governance through national-security mechanisms.[144] Contractual mitigation agreements and statutory screening tools reshape the architecture within which platforms operate, without prescribing substantive moderation outcomes.[145]

These models reflect distinct placements of sovereign power within the platform ecosystem: operator identity in China, distribution access in the UAE, and infrastructural control in the United States. Each approach uses contract to embed authority at a different point in the lifecycle of platform operation.

B. Contractual Instruments and Their Sovereign Function

Although all three systems rely on contract, the function of contractual instruments differs across jurisdictions. Contract serves not as a uniform governance tool, but as a mechanism adapted to each system's legal and institutional constraints.

In China, contract functions as a mechanism of statutory execution. Licensing rules prevent foreign firms from operating directly, requiring them to enter into arrangements with domestic entities that can assume regulatory obligations.[146] These agreements allocate responsibility for compliance with censorship, data-localization, and access requirements.[147] Contract thus operates as the interface through which public-law mandates become technically and organizationally enforceable.

In the UAE, contract functions as a mechanism of conditional access. Carrier agreements do not impose continuous obligations on platforms; instead, they embed platforms within infrastructure through which the State can exercise leverage.[148] Compliance is not specified in advance but is secured through the credible possibility of intervention.[149] Contract, in this context, enables discretionary governance without requiring constant regulatory action.

In the United States, contract functions as a mechanism of structural filtering. Through CFIUS mitigation agreements and related instruments, the government restructures ownership and data governance to address national-security risks.[150] These agreements do not regulate content directly; they determine who may access data, who may control systems, and how corporate

144. U.S. Const. amend. I; Miami Herald Publ'g Co. v. Tornillo, 418 U.S. 241, 258 (1974); 50 U.S.C. § 4565.

145. 50 U.S.C. § 4565; FIRRMA, supra note 96; Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, supra note 102, at 1637–38.

146. Telecommunications Regulations arts. 7–9; Provisions on the Administration of Foreign-Invested Telecommunications Enterprises art. 6 (China).

147. Cybersecurity Law arts. 24, 28, 37; Data Security Law arts. 21, 27, 30; Personal Information Protection Law arts. 10, 38–40.

148. Federal Decree-Law No. 3 of 2003 arts. 12, 14 (U.A.E.); Telecommunications & Digital Government Regulatory Authority, Internet Access Management Regulatory Policy, supra note 55.

149. Federal Decree-Law No. 34 of 2021 arts. 23–25, 34, 38 (U.A.E.).

150. 50 U.S.C. § 4565; FIRRMA, *supra* note 96.

governance is organized.[151] Contract thus filters the conditions under which platform governance occurs rather than dictating its outcomes.

Across these systems, contract alternately serves as an execution mechanism, a bargaining instrument, and a structural constraint. The variation reflects differences in constitutional structure, regulatory capacity, and the role of infrastructure in each jurisdiction.

C. Moderation Outcomes

Because each system embeds authority at a different point, each produces a distinct modality of content moderation. These differences are not merely variations in degree; they reflect fundamentally different relationships between the State and platform governance.

In China, moderation is continuous and anticipatory. Because the operator is legally responsible for preventing the circulation of prohibited content, filtering and compliance mechanisms are embedded upstream in system architecture.[152] Moderation operates as an ongoing condition of service provision rather than as a response to discrete enforcement actions.

In the UAE, moderation is episodic and event-driven. Platforms generally operate without continuous intervention, but enforcement is activated when content implicates political, cultural, or moral concerns.[153] Control over distribution infrastructure enables rapid intervention when needed, while allowing relative autonomy in periods of regulatory dormancy.

In the United States, moderation is indirect and derivative. Government action targets ownership, data access, and technical control rather than content itself.[154] As a result, moderation outcomes emerge from the structural conditions within which platforms operate, rather than from directives specifying what content must be removed or retained.

These differences highlight that digital sovereignty is not exercised solely through the articulation of rules governing speech. It is also exercised through the design of systems that determine how speech is produced, distributed, and controlled. Contractual arrangements play a central role in this process by embedding sovereign authority into the operational foundations of digital platforms.

Conclusion

Digital sovereignty is increasingly exercised through the structural conditions that govern how platforms operate, rather than solely through formal rules that govern what platforms may say or display. Across jurisdictions, key decisions affecting the flow of information are embedded not only in statutes or judicial doctrine, but in the arrangements that determine

151. *Id.*

152. Cybersecurity Law arts. 24, 28, 37; Telecommunications Regulations arts. 7–9.

153. Federal Decree-Law No. 34 of 2021 arts. 23–25; Federal Decree-Law No. 55 of 2023 arts. 17, 22.

154. 50 U.S.C. § 4565; FIRRMA, supra note 96; Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, supra note 102.

who may build, operate, and control digital infrastructure.

The comparative analysis of China, the United Arab Emirates, and the United States demonstrates that contractual governance is not a singular phenomenon, but a set of distinct regulatory strategies adapted to different institutional constraints. In China, contractual arrangements operationalize statutory mandates by assigning regulatory responsibility to licensed domestic operators. In the UAE, contractual dependence on state-controlled infrastructure enables discretionary, event-triggered intervention without continuous regulation. In the United States, contractual mitigation and screening mechanisms restructure ownership and data governance to address national-security risks while preserving formal limits on speech regulation.

These models reflect different placements of sovereign authority within the platform ecosystem. Authority may be embedded in the identity of the operator, in control over access to users, or in control over data and technical systems. In each case, however, the State shapes the environment in which platform governance occurs by defining the conditions under which participation in the digital economy is permitted.

This shift has implications for both transparency and accountability. Governance exercised through contract often operates through bilateral arrangements, informal signaling, or institutional processes that are less visible than traditional rulemaking. As a result, significant decisions affecting speech and information flows may occur outside conventional channels of public scrutiny. At the same time, contractual mechanisms allow states to exert influence in domains where direct regulation may be constrained by constitutional doctrine, market structure, or geopolitical considerations.

The emerging landscape suggests that debates over platform governance cannot be confined to questions of content moderation alone. They must also address the infrastructural and contractual arrangements that determine how platforms are constituted and controlled. As states continue to embed authority in these upstream mechanisms, the governance of digital speech will increasingly turn on questions of architecture, access, and control rather than on the articulation of substantive rules.