

Digital Sovereignty and Non-market Strategy in Multinational Technology Firms: Implications for Asia

Yonglin Zhang

¹UNSW Sydney

Dezhi Zhang

z5387591@zmail.unsw.edu.au

¹UNSW Sydney

Article

Keywords: digital sovereignty, non-market strategy, digital policy, innovation governance, platform governance, Asia

Posted Date: September 21st, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10680698/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Digital Sovereignty and Non-market Strategy in Multinational Technology Firms: Implications for Asia

Abstract

Digital sovereignty has become a defining institutional challenge for multinational technology firms, **reshaping** how digital services are designed, deployed, and governed across jurisdictions. This study examines how four major technology firms—Alphabet/Google, Microsoft, Apple, and Alibaba Cloud—adapt to fragmented sovereignty demands across the European Union, Asia, and other regions. Through a comparative, source-anchored analysis of nine firm-regulatory event sequences from 2018 to 2025, we show that non-market adaptation extends beyond political engagement to include compliance architecture, certification, localization, sovereign-cloud partnerships, trust documentation, and transparency mechanisms. Our findings demonstrate that product architecture systematically conditions the adaptation mix: cloud-infrastructure providers emphasize certification and localization, whereas platform and integrated ecosystem firms place greater weight on political engagement, privacy design, and legitimacy claims. The analysis also reveals a pronounced geographic pattern: in Asia-anchored sequences, market access is resolved through operational architecture rather than political expenditure, underscoring the centrality of credible assurance design for digital innovation governance in the region. These findings extend non-market strategy research, conceptualize digital sovereignty as a policy condition of innovation, and offer implications for firms and policymakers navigating Asia's rapidly evolving digital governance landscape.

Keywords: digital sovereignty; non-market strategy; digital policy; innovation governance; platform governance; Asia

1. Introduction

Digital sovereignty has become a critical challenge for multinational technology firms in the face of accelerating regulatory and geopolitical fragmentation (Luo, 2022; Meyer et al., 2023). Recent scholarship shows that cross-border digital activity increasingly concentrates institutional risk at the level of the firm, particularly where data, cloud infrastructure, artificial intelligence services, platform ecosystems, and cyber security controls underpin both commercial value creation and national capability (Namibians et al., 2019; Yoo et al., 2010). With the digital economy now accounting for roughly 15% of world GDP, global data-Centre traffic quadrupling between 2015 and 2021, and international bandwidth expanding several-hundred-fold since 2002 (International

Data Center Authority, 2025; OECD, 2021, 2025), the institutional terms on which digital services operate have become a first-order strategic concern. Digital innovation scales through technical architecture yet remains subject to institutional permission, so the same service may face markedly different operating conditions across jurisdictions (Meyer et al., 2023).

This study examines these conditions through the lens of digital sovereignty, understood as public authority over the storage, transfer, access, operation, and governance of digital resources. In practice, sovereignty pressure manifests through two intertwined sets of demands: regulatory instruments, understood as formal rules on cross-border transfers, cybersecurity review, cloud procurement, platform conduct, and algorithmic accountability, and legitimacy expectations, referring to political scrutiny of who controls digital infrastructure and on what terms. Regulatory approaches to both differ markedly across the European Union, the United States, China, and Asian economies, creating a persistent gap between technical scalability and institutional scalability (Coche et al., 2024; Luo, 2022; Meyer et al., 2023). Table 1 summaries the principal regulatory logics relevant to the cases.

Table 1. Institutional regimes of digital sovereignty and strategic implications

Jurisdiction	Dominant regulatory logic	Typical policy instruments
United States	Mixed model combining competition, export controls, AI governance debate, industrial policy, sectorial privacy initiatives	Antitrust enforcement, export controls, AI governance debate, industrial policy, sectorial privacy initiatives
European Union	Rights-based and rule-intensive digital governance	GDPR, DMA, DSA, cross-border transfer rules, cloud and competition oversight
China	State-centered and security-oriented digital sovereignty	Data Security Law, Personal Information Protection Law, cyber security review, localization requirements
Developing Asia and Asia-Pacific	Rapid digital transformation with uneven infrastructure and governance capacity	National digital strategies, infrastructure programs, digital inclusion policy, cross-border cooperation

Note. This table summaries regulatory logics without assigning a single fixed regime to all policy areas within each jurisdiction.

For multinational technology firms, this fragmentation reshapes product design, infrastructure planning, and legitimacy management. Firms that rely on cloud services, advertising platforms, app stores, operating systems, data analytics, and artificial intelligence tools are directly exposed

to these demands and urgently need to integrate the sovereignty dimension into their innovation and infrastructure strategies. The resulting strategic question is managerial as well as legal: how can a global digital architecture remain innovative when the institutional environment requires jurisdiction-specific control? Answering it requires choices about centralization, localization, certification, public-authority engagement, partnerships, and trust claims.

Non-market strategy research provides the natural analytical starting point, because firms compete simultaneously in product markets and institutional arenas: corporate political activity, policy engagement, legitimacy management, and organizational responses to institutional pressure are known to affect market access and operating conditions (Baron, 1995; Dahan et al., 2006; Hillman et al., 2004; Mellahi et al., 2016; Oliver, 1991). Digital sovereignty extends this logic into technical architecture itself, as firms reconfigure cloud regions, encryption-key custody, compliance controls, data centers, and local partnerships. Although this literature has grown considerably, it offers limited guidance on how political and architectural responses combine in practice, and few studies explain why firms facing similar sovereignty pressure adopt markedly different mechanism mixes. This paper addresses that gap through a comparative, source-anchored analysis of firm-level adaptation.

Against this background, the study aims to address three interrelated research questions:

1. how digital sovereignty fragmentation shapes the breadth and intensity of non-market adaptation (RQ1);
2. how institutional capability and product architecture condition the mix of adaptation mechanisms that firms deploy (RQ2);
3. how these adaptations, in turn, affect the viability of innovation governance across market access, infrastructural flexibility, and institutional legitimacy (RQ3).

These questions are examined through a structured comparison of Alphabet/Google, Microsoft, Apple, and Alibaba Cloud, four firms selected because they share sustained exposure to digital sovereignty pressure while differing systematically along the dimensions that the framework identifies as decisive: home-country institutional origin, institutional capability, and product architecture. Their configurations span the relevant spectrum: Alphabet/Google combines platform and cloud businesses; Microsoft pairs enterprise software with cloud infrastructure; Apple operates an integrated hardware–software–services ecosystem; and Alibaba Cloud is an Asian-origin cloud-infrastructure provider expanding abroad under geopolitical scrutiny. Although analytically distinct, these configurations overlap in practice, and it is precisely the combination of shared exposure and contrasting architecture that allows the comparison to trace how the same institutional pressure is translated into different strategic responses by platform, infrastructure, and ecosystem firms.

Methodologically, the analysis combines process tracing with a structured archival event design. The primary unit of analysis is a firm-regulatory event sequence comprising a regulatory trigger, an observable firm response, and an innovation-governance implication. The four cases support mechanism analysis and analytical generalization; they do not constitute a statistical sample. Transparent coding formulas, source hierarchy, triangulation, and negative-evidence checks strengthen the auditability of the qualitative inference (Aguinis & Solarino, 2019; Beach & Pedersen, 2019; Collier, 2011). This study makes three contributions:

1. Extends non-market strategy research by showing that, under fragmented sovereignty regimes, firm action runs through compliance architecture, certification, localization, sovereign-cloud partnerships, and trust documentation in addition to political engagement.
2. Conceptualize digital sovereignty as a policy condition that shapes the organization and legitimacy of digital innovation.
3. Explain how product architecture determines the feasible response repertoire and, therefore, the implementation effects of digital policy in the Asian markets foregrounded in this study.

The remainder of the article is organized as follows. Section 2 develops the theoretical background and propositions. Section 3 describes the methods and data. Section 4 presents the within-case findings and the cross-case assessment. Section 5 discusses theoretical contributions and policy implications for Asia, and Section 6 concludes.

2. Theoretical and propositions

2.1. Digital sovereignty as institutional fragmentation

Digital governance research shows that digital exchange is governed through control, coordination, incentive, and trust mechanisms (Hanisch et al., 2023). These mechanisms are increasingly territorial. States increasingly seek to determine where data are stored, who can access them, whether foreign law can compel disclosure, how platforms rank or monetize content, and whether cloud infrastructure can sustain public-sector services under crisis conditions. Digital sovereignty therefore reflects the interaction of formal law, procurement standards, geopolitical concern, and public legitimacy.

International business research has long emphasized that multinational enterprises operate across heterogeneous institutions. Digital businesses intensify that problem because technical systems are scalable but regulatory legitimacy remains territorially bounded (Meyer et al., 2023). A cloud service can be deployed across regions, but the legality and acceptability of data processing may depend on national rules. A platform can standardize user experience globally, but competition authorities may impose jurisdiction-specific gatekeeper duties. A smartphone ecosystem can be designed centrally, but data localization and public-security mandates may require local operational compromises. Digital sovereignty thus creates a gap between technical scalability and institutional scalability.

Fragmentation has three observable components. Regulatory heterogeneity captures differences in rules on data storage, transfer, cyber security, platform conduct, and public-sector cloud procurement. Institutional uncertainty captures changing interpretations, enforcement exposure, and policy shifts. Political exposure captures vulnerability to geopolitical intervention, home-state suspicion, and security review. Firms respond to the combined legal, political, and legitimacy demands created by these components.

2.2. Non-market adaptation in digital industries

Non-market strategy research examines lobbying, campaign contributions, coalition formation, policy engagement, and complementary legitimacy practices (Hillman et al., 2004; Henisz & Zelner, 2012; Liedong et al., 2017; Mellahi et al., 2016). In digital industries, however, the repertoire extends to organizational and technical adaptation. Firms establish privacy and compliance offices, design trust centers, obtain certifications, create data-residency options, negotiate sovereign-cloud partnerships, open local data centers, and publish transparency materials.

The distinction matters for theory. A firm may spend heavily on lobbying and still lose market access if it lacks credible operational controls. Conversely, a firm with strong certification and localization capability may preserve access even in politically sensitive markets. Non-market adaptation under digital sovereignty is therefore both political and architectural. It requires organizational routines that connect legal analysis, technical design, government relations, public communication, and market strategy.

We define non-market adaptation as deliberate organizational action to manage the institutional environment of digital operations. The construct has four mechanisms. Political engagement captures lobbying, consultation participation, policy advocacy, and engagement with regulators. Compliance certification captures formal evidence that a firm meets standards such as information-security, privacy, and data-residency requirements. Localization captures data centers, local operating entities, local cloud regions, sovereign-cloud designs, and host-country partnerships. Legitimacy building captures transparency reports, privacy-by-design features, trust centers, public explanations of legal exposure, and visible commitments to responsible data governance. Because fragmentation raises the combined legal, political, and legitimacy demands on firms, broader fragmentation should be met with a broader adaptation repertoire. We therefore propose:

Proposition 1. Greater digital sovereignty fragmentation is associated with broader and more intensive non-market adaptation by multinational technology firms.

2.3. Innovation-governance viability

Innovation governance refers to the arrangements that enable, constrain, coordinate, and legitimize innovation. In digital firms, these arrangements include internal development choices and the rules that permit products and infrastructures to operate across jurisdictions (Hanisch et al., 2023; Tiwana et al., 2010; Yoo et al., 2010). Three dimensions are central: market access, infrastructural flexibility, and institutional legitimacy.

Digital sovereignty can undermine innovation-governance viability by fragmenting deployment, increasing duplication, and weakening interoperability. It can also strengthen viability when it creates clearer trust expectations and encourages firms to build stronger accountability systems. The direction of the effect depends on the firm's adaptation capability and the fit between

regulatory demands and product architecture. Non-market adaptation is the mechanism through which firms manage this tension. We therefore propose:

Proposition 2. Non-market adaptation links digital sovereignty fragmentation to innovation-governance viability by supporting market access, infrastructural flexibility, and institutional legitimacy.

2.4. Institutional capability as a conditioning factor

Institutional capability is the firm's capacity to interpret, engage with, and adapt to institutional demands. It includes regulatory expertise, compliance architecture, certification portfolios, audit routines, government-relations capability, and experience with public-sector customers. Stronger capability supports earlier and more diversified responses by connecting legal analysis, technical design, government relations, and market strategy. We therefore propose:

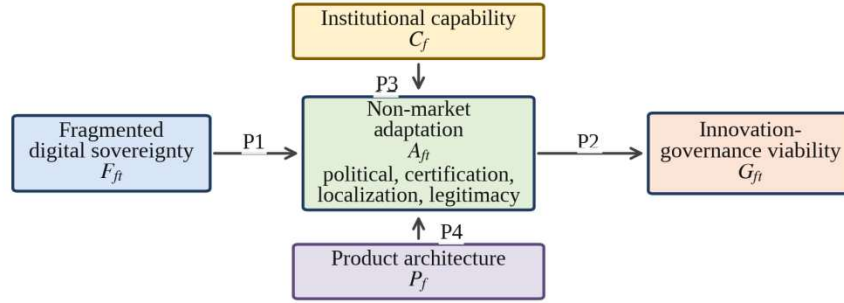
Proposition 3. Institutional capability conditions the response to digital sovereignty fragmentation; firms with mature compliance and government-relations systems use more diversified and proactive adaptation mechanisms.

2.5. Product architecture and the adaptation repertoire

Product architecture shapes both regulatory exposure and the feasible response repertoire, and it does so asymmetrically across the three configurations examined here. Infrastructure providers face direct demands for data location, operational control, certification, service resilience, and public-sector procurement, which channel their adaptation towards certification, localization, and sovereign-cloud engineering. Platform firms are instead exposed to platform conduct, advertising, data use, competition, and user trust, so their responses centre on political engagement, privacy controls, and governance narratives. Integrated ecosystem firms confront a dual problem: they must maintain centralized product control while complying with local demands on app stores, data, devices, and security applications, a tension that pushes them to combine selective localization with the defense of ecosystem integrity. We therefore propose:

Proposition 4. Product architecture shapes the adaptation mix: infrastructure providers emphasize certification and localization, whereas platform and integrated ecosystem firms place greater weight on political engagement, privacy design, and legitimacy claims.

Figure 1 summarizes the proposed relationships among the coded constructs: sovereignty fragmentation, the four non-market adaptation mechanisms, institutional capability, product architecture, and innovation-governance viability. Proposition 1 speaks directly to RQ1; Propositions 3 and 4 develop the conditioning logic at the Centre of RQ2; and Proposition 2 addresses the governance outcome raised by RQ3.



Note. f indexes firm and t indexes event year. The framework guides process tracing and descriptive coding rather than population-level regression.

Figure 1. Theoretical framework and coded constructs.

3. Methods and data

3.1. Research design

This study uses an archival multiple-case design with structured, focused comparison and process tracing (Eisenhardt, 1989; Eisenhardt & Graebner, 2007; George & Bennett, 2005; Langley, 1999; Siggelkow, 2007; Yin, 2018). The design fits a mechanism-oriented research question. It does not estimate a population-level average treatment effect. Instead, it uses transparent firm-regulatory event sequences to examine how digital sovereignty pressure is associated with non-market adaptation and innovation-governance viability.

The unit of analysis is the firm-regulatory event sequence, denoted by k^* . Each sequence contains a regulatory trigger, an observable firm response, and an innovation-governance implication:

$$R_{k^*} \rightarrow A_{k^*} \rightarrow G_{k^*} \quad (1)$$

Equation (1) represents the temporal logic of each sequence. A trigger may be a law, enforcement action, court decision, procurement requirement, security mandate, or geopolitical scrutiny. A response may be lobbying, legal challenge, certification, localization, partnership, transparency reporting, technical redesign, or public communication. A governance implication concerns market access, infrastructural flexibility, or institutional legitimacy. This event-sequence definition improves evidentiary discipline because each claim must be tied to a temporal order and to a source category reported in the supplementary material.

The study period is 2018 through 2025. The period begins with the implementation of the General Data Protection Regulation and Apple's China I Cloud localization, extends through Schrems II and the emergence of transfer uncertainty, and includes more recent sovereignty-by-design strategies such as Microsoft's EU Data Boundary and sovereign-cloud partnerships in Asia. The period therefore captures both early localization responses and more recent architecture-based non-market strategy. The final catalogue comprises nine firm-regulatory event sequences: three for Microsoft, three for Alphabet/Google, two for Apple, and one for Alibaba Cloud (Table 2; source URLs in Supplementary Table S5).

Table 2. Event-sequence catalogue: regulatory triggers, firm responses, and primary mechanisms, 2018–2025

Firm	Year	Regulatory trigger	Observable firm response	Primary mechanism
Apple	2018	China cyber security and localization requirements	GCBD operation of mainland China I Cloud services	Localization and legitimacy tradeoff
Alphabet / Google	2019	CNIL GDPR enforcement and EU privacy pressure	Privacy and consent changes; intensified policy engagement	Political engagement and legitimacy building
Microsoft	2020	Schrems II and transatlantic data-transfer uncertainty	Expanded trust-Centre and European data-residency commitments	Compliance and localization
Microsoft	2021	EU public-sector and enterprise data-residency concerns	EU Data Boundary programme	Localization and trust documentation
Alphabet / Google	2023	Singapore sensitive-workload and sovereign-cloud demand	Google Distributed Cloud Hosted pilot with CSIT	Sovereign-cloud partnership

Firm	Year	Regulatory trigger	Observable firm response	Primary mechanism
Alibaba Cloud	2023	Southeast Asian data governance and geopolitical scrutiny	Local data centers and compliance centers across ASEAN	Certification and localization
Microsoft	2025	EU data-residency and cloud sovereignty pressure	Completion of EU Data Boundary for major cloud services	Infrastructure-based adaptation
Apple	2025	Indian cyber-safety pre installation mandate	Resistance based on privacy and system-security concerns; mandatory rule withdrawn	Ecosystem control and legitimacy building
Alphabet / Google	2025	EU platform and competition oversight	Legal and policy engagement with platform-governance obligations	Political engagement and legitimacy building

Note. Source URLs anchoring each sequence are reported in Supplementary Table S5.

3.2. Case selection

The cases were selected for theoretical variation. Alphabet/Google, Microsoft, Apple, and Alibaba Cloud are all large data-intensive technology firms exposed to privacy, cloud, cyber security, platform, competition, and cross-border data issues. They differ on two theoretical dimensions. The first is home-country institutional origin: three are U.S.-headquartered firms, whereas Alibaba Cloud is headquartered in China and operates abroad under different geopolitical assumptions. The second is product architecture: Alphabet/Google combines platform and cloud activities; Microsoft is a major enterprise software and cloud-infrastructure firm; Apple is an integrated ecosystem firm; and Alibaba Cloud is a cloud-infrastructure provider with strong Asian market exposure.

This selection follows theoretical replication logic. Similar sovereignty pressure should be associated with common expansion in adaptation breadth, while different product architectures should be associated with different mechanism mixes. The comparison supports analytical pattern matching rather than statistical hypothesis testing.

3.3. Data sources

The evidence base consists of public and replicable archival sources. Legal and regulatory materials include the GDPR, the Schrems II judgment, EU platform and competition decisions, Chinese cyber security and data rules, and the Indian smartphone cyber-safety mandate examined in the Apple sequence (Court of Justice of the European Union, 2020; European Parliament & Council of the European Union, 2016; Reuters, 2025a, 2025b, 2025c). Firm-level materials include trust centers, transparency reports, China iCloud terms, sovereign-cloud announcements, compliance centers, annual reports, and policy statements (Apple Inc., 2024; Google Cloud, 2023; Microsoft, 2025). Political-engagement data are drawn from Open Secrets (2024a, 2024b, 2024c). Peer-reviewed research anchors the constructs and supports triangulation.

Industry reports are used only as contextual benchmarks when the data point and issuing organization are explicit. They are excluded from causal evidence. The contextual indicators in Figure 2 use the IDCA Global Digital Economy Report (International Data Centre Authority, 2025) and OECD evidence on data-Centre traffic and international bandwidth (OECD, 2021, 2025). The source hierarchy separates official materials, firm disclosures, peer-reviewed scholarship, political-engagement records, and industry commentary; Table 3 summarizes these source categories, their construct roles, and their evidentiary status.

Table 3. Data sources, construct role, and evidentiary status

Source category	Examples used in the study	Construct role	Evidentiary status
Official legal and regulatory materials	GDPR, Schrems II, EU platform and competition decisions, China data laws, Indian cyber-safety mandate and withdrawal	Regulatory trigger and fragmentation coding	Highest-priority source for legal and policy events.
Firm disclosures and trust documentation	Microsoft EU Data Boundary materials, Google Cloud sovereign-cloud announcements, Apple	Firm response and institutional capability coding	Primary source for observable firm adaptation.

Source category	Examples used in the study	Construct role	Evidentiary status
	China I Cloud terms, Alibaba Cloud compliance and data-Centre materials		
Political-engagement records	Open Secrets 2024-cycle lobbying records for Alphabet, Microsoft, and Apple	Political-engagement indicator	Public disclosure dataset; used descriptively and validated against public summaries.
Peer-reviewed scholarship	Studies on data governance, non-market strategy, process methods, digital international business, privacy responses, and Chinese cloud providers in Southeast Asia	Theory, construct definition, triangulation, and mechanism interpretation	Used to anchor interpretation and avoid reliance on press commentary alone.
Industry and public benchmark sources	IDCA and OECD source-identified indicators	Context and descriptive charts	Treated as contextual support, not causal evidence.

Note. The empirical claims rely on public and replicable sources and exclude proprietary interviews and synthetic data. Source hierarchy and coding rules are reported in the supplementary material.

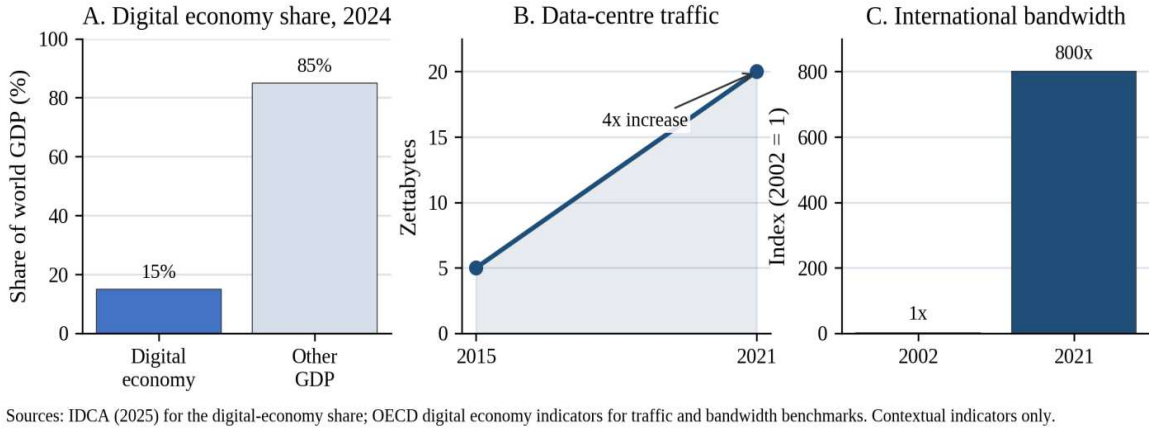


Figure 2. Contextual benchmarks for digital economy scale and infrastructure growth.

3.4. Measures and coding

The coding scheme uses ordinal measures to discipline comparison while keeping the primary inference process-based. For firm f and event year t , digital sovereignty fragmentation is defined as the mean of three source-supported indicators: transfer restrictions T_{ft} , enforcement exposure E_{ft} , and geopolitical exposure P_{ft} . Each indicator is coded on an anchored scale from 0 to 2:

$$F_{ft} = (T_{ft} + E_{ft} + P_{ft}) / 3 \quad (2)$$

Non-market adaptation is defined as the breadth of four mechanisms: political engagement L_{ft} , compliance certification C_{ft} , localisation D_{ft} , and legitimacy building R_{ft} . Each mechanism is coded as an event-level count or anchored intensity score, depending on the available source type. The adaptation breadth score is:

$$A_{ft} = L_{ft} + C_{ft} + D_{ft} + R_{ft} \quad (3)$$

Innovation-governance viability is assessed across market access M_{ft} , infrastructural flexibility I_{ft} , and institutional legitimacy Q_{ft} . The governance score is:

$$G_{ft} = (M_{ft} + I_{ft} + Q_{ft}) / 3 \quad (4)$$

The coded evidence is also summarized at the firm level. For a firm with n_f coded event sequences, the mean adaptation breadth is:

$$\bar{A}_f = (1 / n_f) \sum A_{fk} \quad (5)$$

Equations (2)-(5) define descriptive codes. They make qualitative comparison auditable by applying common coding anchors across cases. They do not convert the case evidence into independent observations or provide inferential estimates. Table 4 consolidates the constructs, formulas, and their interpretation. The supplementary material reports the source-anchored event catalogue, coding anchors, and source URLs.

Table 4. Construct formulas and interpretation

Construct	Formula	Interpretation	Primary use
Sovereignty fragmentation	$F_{ft} = (T_{ft} + E_{ft} + P_{ft}) / 3$	Mean exposure to transfer restrictions, enforcement exposure, and geopolitical exposure	Institutional condition
Non-market adaptation breadth	$A_{ft} = L_{ft} + C_{ft} + D_{ft} + R_{ft}$	Breadth of political engagement, compliance certification, localisation	Adaptation mechanism

Construct	Formula	Interpretation	Primary use
		on, and legitimacy building	
Innovation-governance viability	$G_{ft} = (M_{ft} + I_{ft} + Q_{ft}) / 3$	Mean viability across market access, infrastructure flexibility, and institutional legitimacy	Governance outcome
Firm-level mean adaptation	$\bar{A}_f = n_f^{-1} \sum A_{fk}$	Average event-sequence adaptation breadth within a case	Firm-level descriptive diagnostic

Note. The formulas reproduce Eqs. (2)-(5) to make the descriptive coding auditable.

3.5. Analytical procedure

The analysis proceeded in four steps. First, within-case chronologies identified regulatory triggers, public responses, technical or organizational adaptation, and governance implications. Second, event-level coding applied the source hierarchy and anchored coding rules. Third, cross-case pattern matching compared mechanism choices across product architectures. Fourth, negative evidence was examined by searching for high sovereignty pressure without observable adaptation and strong adaptation without governance relevance.

Figures 3 through 5 are descriptive diagnostics. Figure 3 compares the mechanism mix across cases. Figure 4 reports the cross-case coding matrix. Figure 5 reports lobbying expenditures for the U.S.-headquartered focal firms. These visuals support pattern matching and source transparency without reporting statistical significance.

4. Findings

The findings proceed in three steps. Sections 4.1–4.4 reconstruct the within-case event sequences; Section 4.5 develops the cross-case comparison against the coded evidence; Section 4.6 assesses each proposition. Throughout, coded values are read as descriptive diagnostics that discipline comparison, not as inferential estimates.

4.1. Microsoft: Data Boundary as infrastructure-based non-market strategy

Microsoft's case shows how a cloud and enterprise-software firm converts digital sovereignty pressure into infrastructure-based adaptation. GDPR implementation, the Schrems II judgment, and public-sector concern about foreign legal access created sustained pressure for European data residency (Court of Justice of the European Union, 2020; European Data Protection Board, 2020). Microsoft responded through the EU Data Boundary and announced its completion for major cloud services in 2025 (Microsoft, 2025).

This sequence supports Propositions 1 and 2. Escalating fragmentation broadened the adaptation repertoire, and regulatory pressure produced operational adaptation that preserved market access and improved institutional legitimacy for public-sector and enterprise customers. Microsoft also maintained political engagement through substantial U.S. federal lobbying expenditures in the 2024 cycle. The distinctive response was architectural: the EU Data Boundary made data-residency assurance a service feature.

The Microsoft case also supports Proposition 4. As an infrastructure provider, Microsoft could adapt by localizing storage and processing, publishing trust documentation, and creating

evidence of data-residency controls. That response differs from platform-centered political engagement because the customer value proposition is itself tied to assurance, procurement eligibility, and compliance readability. The product architecture therefore shaped the mechanism of adaptation. In the coded matrix, Microsoft combines the highest certification and localization intensities among the U.S.-headquartered cases (3 and 3) with the lowest political-engagement score among them (1) and a governance-viability score of 3 (Figure 4).

4.2. Alphabet/Google: Dual adaptation across platform and cloud activities

Alphabet/Google faces a broad set of sovereignty pressures because its business spans search, advertising, mobile operating systems, cloud services, artificial intelligence, and digital platforms. A 2019 enforcement decision by the French data protection authority made transparency and consent a central legitimacy issue, while EU platform oversight and cross-border transfer requirements expanded the policy exposure (Commission nationale de l'informatique et des libertés, 2019).

Google's response combines political engagement with cloud-specific structural adaptation. Open Secrets reports substantial U.S. federal lobbying expenditure, while sovereign-cloud partnerships provide localized operational control. In 2023, Google Cloud and Singapore's Centre for Strategic Infocomm Technologies announced a Google Distributed Cloud Hosted pilot for sensitive workloads in an isolated environment (Google Cloud, 2023; Open Secrets, 2024a).

The case supports Proposition 1 because rising fragmentation is associated with a broader adaptation repertoire. It also supports Proposition 4 because Alphabet/Google's response is mixed. Its platform business requires political engagement and data-use legitimacy. Its cloud business requires certification, residency, and sovereign-cloud options. Mixed product architecture therefore creates a dual non-market strategy. Alphabet/Google is the only case coded at the maximum on both transfer restrictions and enforcement exposure (2 and 2), and its adaptation profile is uniformly broad, with a score of 2 on every mechanism (Figure 4).

4.3. Apple: Ecosystem control and selective localization

Apple's case illustrates the tension between ecosystem integrity and jurisdiction-specific sovereignty demands. In China, Apple transferred mainland iCloud operations to Guizhou-Cloud Big Data Industry Development Co., Ltd.; the service terms identify GCBD as the operator for mainland China (Apple Inc., 2024; Reuters, 2018). This arrangement preserved market access while relocating data governance to the local legal environment.

Apple's later interaction with India shows a second ecosystem response. In 2025, the government directed smartphone manufacturers to preload the Sanchar Saathi cyber-safety application. Reuters reported that Apple planned to resist on privacy and system-security grounds; the

government subsequently withdrew the mandatory reinstallation requirement (Reuters, 2025a, 2025b, 2025c).

The Apple case supports Proposition 4. Integrated ecosystem architecture creates high sensitivity to mandatory reinstallation, app-store rules, data custody, and device-level control. Apple therefore uses a selective strategy: localized compliance in China, visible privacy and security claims in India, and political engagement where policy issues affect ecosystem governance. Innovation governance depends on preserving the integrity of the ecosystem while meeting jurisdiction-specific requirements. Apple's coded profile pairs the highest legitimacy-building score in the corpus (3) with the lowest certification score (1), consistent with an ecosystem strategy that privileges trust claims over auditable compliance evidence (Figure 4).

4.4. Alibaba Cloud: Offshore embeddedness and certification-heavy adaptation

Alibaba Cloud provides an Asian-origin perspective on digital sovereignty. As a Chinese cloud provider operating abroad, it faces host-market concerns about data access, foreign control, and geopolitical dependency. Its response emphasizes local data centers, certifications, partnerships, and compliance evidence, a pattern described as offshore embeddedness (Alibaba Cloud, n.d.; Yang & Li, 2025).

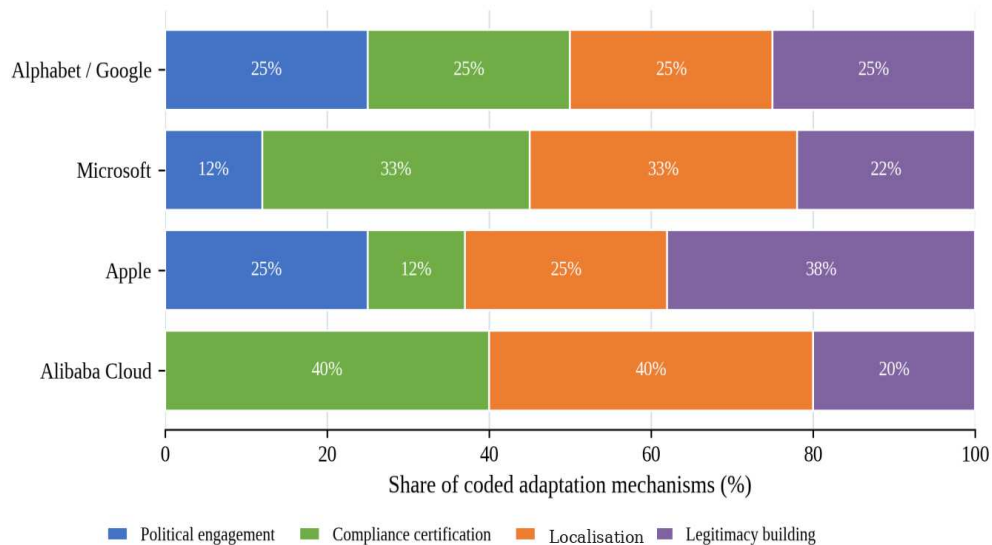
The firm's Southeast Asian expansion illustrates the mechanism. Alibaba Cloud operates data-Centre regions and compliance services across Southeast Asian markets. Yang and Li (2025) document how host-market embedding and certification support legitimacy under data-localization, licensing, and security-audit requirements.

This case supports Proposition 3. Alibaba Cloud faced regulatory heterogeneity and geopolitical exposure. Its response relied on institutional capability expressed through certifications, local data centers, and host-market compliance evidence. The case also supports Proposition 4 because infrastructure architecture made compliance evidence and local operational presence the most salient adaptation mechanisms. Alibaba Cloud's coded profile is the most polarized in the corpus: maximum intensities for certification and localization (4 and 4), no coded political engagement (0), and, together with Apple, the highest geopolitical-exposure score (2) (Figure 4).

4.5. Cross-case patterns: product architecture shapes the adaptation mix

The cross-case evidence supports the proposed model; Table 5 summaries each case's regulatory exposure, observable response, and governance implication. All four firms intensified non-market adaptation under sovereignty fragmentation, but they did so through different mechanisms. Microsoft and Alibaba Cloud relied most heavily on localization, certification, and trust-Centre evidence; Alphabet/Google pursued a hybrid strategy reflecting an architecture that spans platforms and cloud infrastructure; and Apple protected ecosystem control through selective localization and privacy-based legitimacy. Figure 3 summarises the mechanism mix, and Figure 4 reports the source-anchored coding matrix underlying the pattern-matching

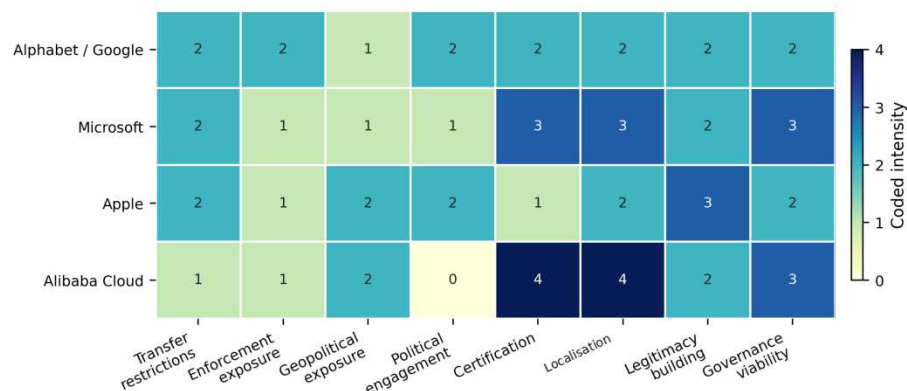
assessment. Read as descriptive diagnostics rather than estimates, the coded profiles differ more in composition than in total breadth: adaptation breadth ranges narrowly from 8 (Alphabet/Google and Apple) to 10 (Alibaba Cloud), while the distribution across mechanisms varies sharply with product architecture.



Note. Mechanism counts are based on the firm-event catalogue in Table 2 of the main text. Percentages are shown for pattern matching.

Figure 3.

Mechanism mix by product architecture.



Note. Scale anchors differ by construct and are reported in Supplementary Tables S2-S4. The matrix is used to discipline comparison, not to estimate statistical effects.

Figure 4.

Cross-case coding matrix for source-anchored pattern matching.

Table 5. Comparative case summary: digital sovereignty pressure and firm response

Firm	Main regulatory exposure	Observable non-market response	Innovation-governance implication	Asia-relevant lesson
------	--------------------------	--------------------------------	-----------------------------------	----------------------

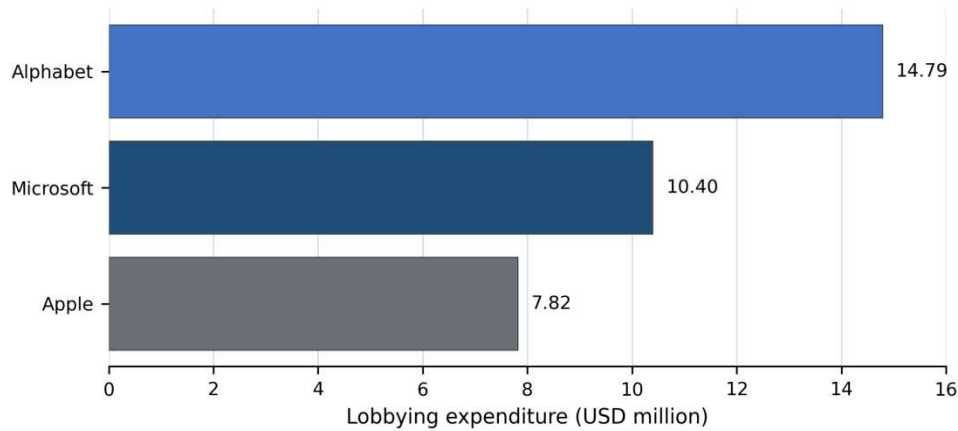
Firm	Main regulatory exposure	Observable non-market response	Innovation-governance implication	Asia-relevant lesson
Alphabet / Google	Privacy, antitrust, platform oversight, AI governance, cross-border data rules	High-intensity lobbying combined with sovereign-cloud partnerships in Asia	Seeks to preserve ecosystem scalability while maintaining trust in cloud services	Platform firms in Asian markets must invest early in credible compliance communication.
Microsoft	Cloud regulation, AI governance, enterprise compliance, antitrust	EU Data Boundary completion, trust-Centre compliance, and sustained lobbying	Supports trusted institutional positioning in enterprise and public-sector markets	Standards compatibility and regulatory readability matter for digital innovation.
Apple	Privacy, app ecosystem regulation, trade pressure, competition policy	Selective lobbying, GCBD localization in China, and resistance to device-level reinstallation mandates	Defends ecosystem control while reinforcing a trust premium	Innovation advantage depends on institutional legitimacy and design capability.
Alibaba Cloud	Chinese digital sovereignty and cross-border	Certification-heavy adaptation and local data centers across	Uses compliance capability to support	Asian firms may convert compliance capability into a strategic asset.

Firm	Main regulatory exposure	Observable non-market response	Innovation-governance implication	Asia-relevant lesson
	compliance demands	ASEAN	legitimacy and market access abroad	

Note. The table reports mechanism-level evidence and not exhaustive legal history. Monetary lobbying amounts used in Figure 5 are based on Open Secrets 2024-cycle records.

The cases do not support a compliance-cost-only interpretation. Firms did more than resist regulation or absorb administrative burden. Microsoft made data-residency pressure part of cloud assurance. Google used sovereign-cloud partnerships to maintain relevance in sensitive public-sector and regulated workloads. Alibaba Cloud used compliance and local data-centre presence to reduce geopolitical distrust. Apple used privacy and system-security claims to resist device-level intervention while accepting localization where market access required it.

The cases also limit a lobbying-only interpretation of non-market strategy. Lobbying is visible and important for U.S.-headquartered firms, but operational evidence drives several outcomes. Infrastructure firms rely heavily on certification, residency controls, and auditability. Ecosystem firms rely on product design credibility and user trust. The relevant strategic capability integrates political, technical, and organizational responses. Figure 5 reports lobbying as one indicator of political engagement, and Table 6 juxtaposes it with the coded adaptation profiles. The comparison makes the point concrete: the largest spender in the 2024 cycle, Alphabet (US\$14.79 million), does not record the highest governance-viability score; Microsoft does (3), on roughly two-thirds of that expenditure and the heaviest architectural profile in the U.S.-headquartered group.



Sources: OpenSecrets company records; public summaries in Issue One (2025) and Statista (2025/2026) used to cross-check amounts. *Figure 5.*

U.S. federal lobbying expenditures of selected firms, 2024. The plotted amounts are from Open Secrets company records; public summaries were used only as cross-checks.

Table 6. U.S. federal lobbying expenditure and coded adaptation profile by firm

Firm	Lobbying, 2024 cycle (USD m)	Political engagem ent	Complia nce certificati on	Localizat ion	Legitim acy building	Governa nce viability
Alphab et / Google	14.79	2	2	2	2	2
Micros oft	10.40	1	3	3	2	3
Apple	7.82	2	1	2	3	2
Alibab a Cloud	n/a	0	4	4	2	3

Note. Lobbying amounts are OpenSecrets 2024-cycle company records (Figure 5); coded intensities reproduce the cross-case matrix (Figure 4). OpenSecrets covers U.S. federal lobbying only, so no amount is reported for Alibaba Cloud.

The geography of the event catalogue sharpens the architectural argument (Table 7). Five of the nine sequences are anchored in the European Union and four in Asia (China, Singapore, Southeast Asia, and India). Political engagement appears as a primary mechanism only in EU sequences, whereas every Asia-anchored sequence turns on operational architecture: localization in China, sovereign-cloud design in Singapore, certification-backed embedding in Southeast Asia, and device-level ecosystem control in India. For the Asian markets foregrounded in this study, credible architecture rather than political expenditure is the operative currency of market access.

Table 7. Distribution of event sequences by trigger jurisdiction and primary mechanism

Trigger jurisdiction	Sequences (n)	Firms involved	Primary mechanisms recorded
European Union	5	Alphabet / Google; Microsoft	Political engagement and legitimacy building; compliance and localisation; trust documentation; infrastructure-based adaptation
China	1	Apple	Localisation and legitimacy tradeoff
Singapore	1	Alphabet / Google	Sovereign-cloud partnership
Southeast Asia	1	Alibaba Cloud	Certification and localization
India	1	Apple	Ecosystem control and legitimacy building

Note. Derived from the nine-sequence event catalogue (Table 2). Jurisdiction refers to the public authority issuing the regulatory trigger; mechanisms are recorded as coded in the catalogue.

4.6. Assessing the propositions against the coded evidence

Table 9 consolidates the pattern-matching assessment across the four propositions. Proposition 1 is supported by the common directional pattern: sovereignty fragmentation is associated with

greater breadth of non-market adaptation. The evidence is strongest where firms face multiple simultaneous pressures, such as GDPR enforcement, transfer uncertainty, public-sector cloud requirements, platform oversight, and geopolitical scrutiny.

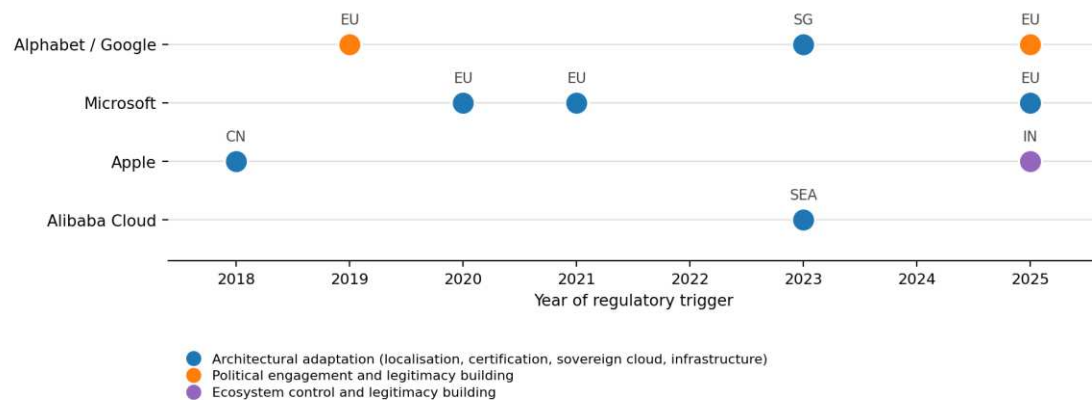
Proposition 2 is supported by the temporal structure of the cases (Table 8; Figure 6). Regulatory triggers preceded firm responses, and responses helped preserve or improve governance viability. Microsoft preserved European enterprise and public-sector cloud access. Google maintained public-sector relevance in Singapore through a sovereign-cloud pilot. Apple maintained China market access through localization and helped preserve ecosystem control when India withdrew mandatory reinstallation. Alibaba Cloud expanded in Southeast Asia by embedding locally and evidencing compliance.

Table 8. Process-tracing evidence by firm-event sequence

Case sequence	Regulatory trigger	Firm response	Governance implication
Microsoft and EU cloud data	GDPR, Schrems II, and public-sector data-residency concerns	EU Data Boundary, trust-Centre documentation, and local storage/processing commitments	Preserved enterprise and public-sector market access by turning residency into an assurance feature.
Google and Singapore sovereign cloud	Public-sector sensitivity regarding defense and security workloads	Google Distributed Cloud Hosted pilot with CSIT in a disconnected environment	Maintained relevance for regulated workloads by offering localized operational control.
Apple and China iCloud	China cyber security and localization requirements	GCBD operation of China mainland iCloud services	Preserved market access through localized operational arrangement while increasing legitimacy tradeoffs.
Apple and India smartphone	Government order to preload a state cyber-safety app	Privacy and system-security resistance; mandate later withdrawn	Helped preserve ecosystem control and reinforced privacy-based

Case sequence	Regulatory trigger	Firm response	Governance implication
mandate		as mandatory reinstallation	legitimacy.
Alibaba Cloud in Southeast Asia	Data-localization, procurement, and geopolitical scrutiny	Local data centers, certifications, compliance centers, and host-market embeddedness	Reduced trust deficit and supported expansion in sovereignty-sensitive cloud markets.

Note. Each row follows the sequence regulatory trigger → firm response → governance implication. The supplementary material provides coding anchors and source documentation.



Note. Derived from the nine-sequence event catalogue (Table 2 of the main text). Labels indicate the trigger jurisdiction: CN = China, EU = European Union, SG = Singapore, SEA = Southeast Asia, IN = India.

Figure 6.

Firm-regulatory event sequences by year, trigger jurisdiction, and primary mechanism class, 2018–2025.

Proposition 3 is supported by variation in institutional capability. Microsoft and Alibaba Cloud show how mature compliance architecture enables proactive adaptation. Microsoft operationalized the EU Data Boundary through enterprise-grade compliance and cloud documentation systems. Alibaba Cloud competed in Southeast Asia through certifications and local data centers that evidenced host-market commitment. Alphabet/Google also shows high capability, although its platform and advertising exposure creates legitimacy risks that certification alone cannot resolve.

Proposition 4 receives the clearest comparative support. Product architecture shapes which adaptation mechanisms are operationally credible. Cloud infrastructure can be localized, certified, audited, and contractually assured. Platforms must address data-use legitimacy and

competition oversight, while integrated ecosystems must protect device and software control while making jurisdiction-specific compromises.

Table 9. Cross-case pattern matching against theoretical propositions

Theoretical proposition	Cross-case pattern	Evidentiary assessment
Proposition 1: Fragmentation is associated with adaptation breadth.	All four firms combine more than one non-market mechanism under sovereignty pressure.	Supported. Evidence is strongest where firms face privacy, transfer, security, and platform pressures simultaneously.
Proposition 2: Adaptation links fragmentation to governance viability.	Adaptation sequences preserve market access or legitimacy in EU, Singapore, China, India, and Southeast Asia events.	Supported. Temporal ordering is consistent across process-tracing cases.
Proposition 3: Institutional capability conditions adaptation.	Microsoft and Alibaba Cloud show proactive certification and localization; Google shows broad capability but higher platform legitimacy exposure.	Supported. Capability changes the timing and diversity of response.
Proposition 4: Product architecture shapes mechanism choice.	Infrastructure firms emphasize certification and localization; platform and ecosystem firms emphasize political engagement, privacy design, and legitimacy.	Strongly supported. Architecture explains response differences under similar sovereignty pressure.

Note. The assessment uses pattern matching and does not claim statistical significance. Scores and coding rules are reported in Supplementary Tables S2-S7.

5. Discussion

5.1. Non-market strategy beyond lobbying: theoretical implications

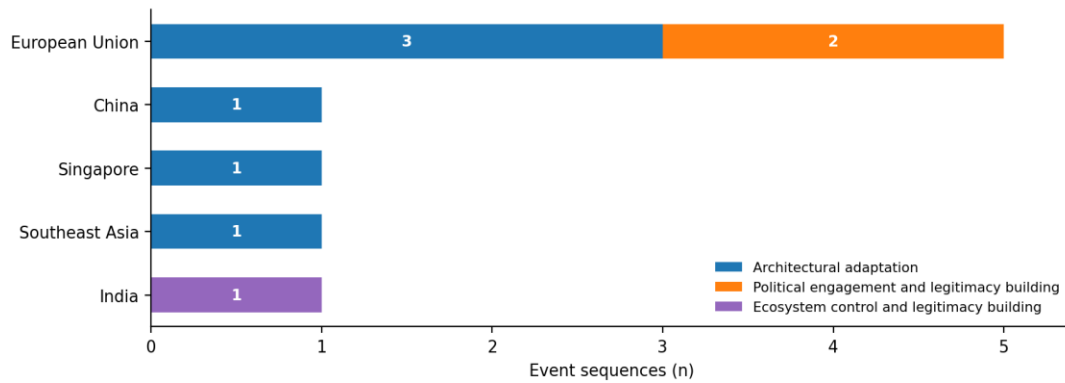
This study contributes to non-market strategy research by expanding the documented repertoire of firm action in digital policy environments. Political engagement remains relevant, but the cases show that compliance architecture, data-residency design, sovereign-cloud partnerships, certification, trust centers, transparency reporting, and privacy engineering also affect market access and procurement eligibility.

The study also contributes to innovation governance. Digital sovereignty constrains innovation when fragmented rules duplicate infrastructure, reduce interoperability, or increase regulatory uncertainty. It can also strengthen governance when it induces firms to build clearer assurance systems, localized infrastructure, and trust mechanisms. Regulation becomes part of the governance architecture of innovation. In sovereignty-sensitive sectors, compliance and legitimacy operate as design conditions.

A third contribution concerns product architecture. Management research on digital platforms and ecosystems often emphasizes scalability, complementarity, and network effects. This study shows that product architecture also determines non-market adaptation. Infrastructure can be localized and certified. Platforms must defend data-use legitimacy and competition practices. Integrated ecosystems must protect architectural control at the device, software, and service levels. The same sovereignty pressure therefore generates different strategic responses because products expose firms to different institutional vulnerabilities.

5.2. Implications for Asia: assurance design as market-access design

Asia is central to the phenomenon because the region combines rapid digitalization, uneven regulatory capacity, and active policy experimentation. Some economies seek global digital infrastructure, while others emphasize data localization, digital public infrastructure, cybersecurity control, or domestic capability. The cases indicate that policy design affects whether sovereignty requirements generate transparent assurance mechanisms or costly fragmentation. The event geography reported in Table 7 and visualized in Figure 7 underscores what is at stake: in every Asia-anchored sequence, market access was resolved through operational architecture rather than political engagement, so the design of assurance requirements directly determines which firms can credibly comply.



Note. Derived from the nine-sequence event catalogue (Table 2 of the main text). Political engagement appears as a primary mechanism only in EU-anchored sequences.

Figure 7.

Distribution of event sequences by trigger jurisdiction and mechanism class.

Three policy implications follow. First, requirements should be transparent, auditable, and consistent across agencies. Second, mutual recognition of cybersecurity, privacy, and cloud-assurance standards can preserve public authority while limiting unnecessary infrastructure duplication. Third, procurement and regulatory frameworks should permit multiple compliance architectures when they provide equivalent protection, including trusted transfer mechanisms, sovereign-cloud configurations, and independently auditable controls.

5.3. Robustness and negative evidence

Table 10 reports five diagnostics that probe the stability of these patterns. Excluding lobbying amounts leaves the infrastructure and certification cases unchanged, indicating that the findings do not depend on political-spending data. Removing the contextual industry indicators does not alter the assessment of any proposition. A targeted negative-case search found no focal case with sustained high sovereignty pressure and no observable response, and adaptation is strongest where governance stakes are highest, a pattern consistent with the proposed mechanism while marking its boundary conditions. Recoding Alphabet/Google as platform-first and Microsoft as infrastructure-first leaves the architecture pattern of Proposition 4 intact. These checks are qualitative and cannot rule out selection effects: all four cases are large incumbents that adapted, so the repertoire of smaller firms, and of firms that exited rather than adapted, remains outside the observed evidence.

Table 10. Robustness and negative-evidence diagnostics

Diagnostic	Procedure	Result	Interpretation
Excluding lobbying amounts	Re-read cases using only operational and	Microsoft and Alibaba Cloud remain infrastructure/certification	Findings do not depend on political spending.

Diagnostic	Procedure	Result	Interpretation
	firm-disclosure evidence	cases; Apple remains an ecosystem-control case	
Excluding contextual industry indicators	Remove Figure 2 from interpretive chain	Propositions and case mechanisms are unchanged	Contextual benchmarks do not drive the causal argument.
Treating press reporting as secondary	Use Reuters only for event chronology when official materials are unavailable or incomplete	India smartphone mandate sequence remains source-supported through multiple dated Reuters reports	Secondary reporting supports chronology, not theory by itself.
Negative case search	Look for high sovereignty pressure without adaptation and high adaptation without governance relevance	No focal case shows sustained high pressure with no observable response; adaptation is strongest when governance stakes are high	Supports mechanism plausibility while preserving boundary conditions.
Alternative mechanism emphasis	Recode Google as platform-first and Microsoft as infrastructure-first	Product architecture still predicts mechanism choice	Supports Proposition 4.

Note. Diagnostics are qualitative re-reading exercises applied to the coded event catalogue; they do not constitute statistical sensitivity tests.

5.4. Boundary conditions, limitations, and future research

The study has three main boundary conditions. The cases are large multinational technology firms with resources that smaller firms may lack. The evidence is limited to publicly observable documents and does not reveal confidential negotiations or internal decision processes. The event-sequence scores are descriptive and support transparent comparison, not statistical estimation. The analysis therefore identifies plausible mechanisms within the selected cases and does not claim that digital sovereignty is the sole determinant of innovation-governance viability.

These limitations also indicate opportunities for future research. Scholars can test the model using larger samples of cloud regions, platform enforcement actions, public-sector procurement awards, or cross-border data-transfer restrictions. Researchers can also examine how firms make build-versus-partner decisions when facing sovereignty demands. Finally, future work can study whether sovereign-cloud and data-localization strategies improve actual user trust or mainly satisfy procurement and regulatory requirements.

6. Conclusion

Digital sovereignty changes where data can be stored, how digital services can operate, which public authorities firms must engage, and what assurance evidence firms must provide. Across the four cases, non-market adaptation includes political engagement, certification, localization, trust documentation, transparency, and sovereign-cloud design.

These findings deliver the three contributions proposed at the outset. First, the study extends non-market strategy research: under fragmented sovereignty regimes, firm action spans compliance architecture, certification, localization, sovereign-cloud partnerships, and trust documentation, and these architectural responses, rather than political spending alone, often determine market access and procurement eligibility. Second, the study conceptualizes digital sovereignty as a policy condition of digital innovation rather than an external constraint. Sovereignty rules shape where infrastructure is built, how services are assured, and which governance claims are credible, so regulation becomes part of the governance architecture of innovation. Third, the study shows that product architecture explains systematic variation in adaptation. Cloud-infrastructure providers can convert residency and certification demands into assurance features, whereas platform and integrated ecosystem firms must defend data-use legitimacy and architectural control. The same sovereignty pressure therefore produces different strategic responses across firms.

Future research can test these relationships using larger samples of cloud regions, platform enforcement actions, procurement decisions, and cross-border transfer restrictions.

References

- Aguinis, H., & Solarino, A. M. (2019). Transparency and replicability in qualitative research: The case of interviews with elite informants. *Strategic Management Journal*, 40(8), 1291–1315. <https://doi.org/10.1002/smj.3015>
- Alibaba Cloud. (n.d.). *Trust center*. Retrieved July 18, 2026, from <https://www.alibabacloud.com/en/trust-center>
- Apple Inc. (2024, September 16). *iCloud operated by GCBD terms and conditions*. <https://www.apple.com/legal/internet-services/icloud/en/gcbd-terms.html>
- Baron, D. P. (1995). Integrated strategy: Market and nonmarket components. *California Management Review*, 37(2), 47–65. <https://doi.org/10.2307/41165788>
- Beach, D., & Pedersen, R. B. (2019). *Process-tracing methods: Foundations and guidelines* (2nd ed.). University of Michigan Press.
- Coche, E., Kolk, A., & Ocelik, V. (2024). Unravelling cross-country regulatory intricacies of data governance: The relevance of legal insights for digitalization and international business. *Journal of International Business Policy*, 7(1), 112–127. <https://doi.org/10.1057/s42214-023-00172-1>
- Collier, D. (2011). Understanding process tracing. *PS: Political Science & Politics*, 44(4), 823–830. <https://doi.org/10.1017/S1049096511001429>
- Commission nationale de l'informatique et des libertés. (2019, January 21). *The CNIL's restricted committee imposes a financial penalty of 50 million euros against Google LLC*. <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-lle>
- Court of Justice of the European Union. (2020). *Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems, Case C-311/18*. <https://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=EN>
- Dahan, N. M., Doh, J. P., & Guay, T. R. (2006). The role of multinational corporations in transnational institution building: A policy-network perspective. *Human Relations*, 59(11), 1571–1600. <https://doi.org/10.1177/0018726706072842>
- Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review*, 14(4), 532–550. <https://doi.org/10.5465/amr.1989.4308385>
- Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal*, 50(1), 25–32. <https://doi.org/10.5465/amj.2007.24160888>

European Data Protection Board. (2020). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*. https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679. *Official Journal of the European Union*, L 119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

George, A. L., & Bennett, A. (2005). *Case studies and theory development in the social sciences*. MIT Press.

Google Cloud. (2023, November 16). *CSIT and Google Cloud collaborate to pilot sovereign cloud solution in Singapore*. <https://cloud.google.com/blog/topics/public-sector/google-cloud-and-csit-collaborate-on-sovereign-cloud-solution>

Hanisch, M., Goldsby, C. M., Fabian, N. E., & Oehmichen, J. (2023). Digital governance: A conceptual framework and research agenda. *Journal of Business Research*, 162, Article 113777. <https://doi.org/10.1016/j.jbusres.2023.113777>

Henisz, W. J., & Zelner, B. A. (2012). Strategy and competition in the market and nonmarket arenas. *Academy of Management Perspectives*, 26(3), 40–51. <https://doi.org/10.5465/amp.2011.0102>

Hillman, A. J., Keim, G. D., & Schuler, D. (2004). Corporate political activity: A review and research agenda. *Journal of Management*, 30(6), 837–857. <https://doi.org/10.1016/j.jm.2004.06.003>

International Data Center Authority. (2025). *Global digital economy report 2025*. <https://www.idc-a.org/insights/qUi9XgvyrzSkyDUy9Tqr>

Langley, A. (1999). Strategies for theorizing from process data. *Academy of Management Review*, 24(4), 691–710. <https://doi.org/10.5465/amr.1999.2553248>

Liedong, T. A., Ghobadian, A., Rajwani, T., & O'Regan, N. (2017). Toward a view of complementarity: Trust and policy influence effects of corporate social responsibility and corporate political activity. *Group & Organization Management*, 42(3), 405–437. <https://doi.org/10.1177/1059601115612174>

Luo, Y. (2022). Illusions of techno-nationalism. *Journal of International Business Studies*, 53(3), 550–567. <https://doi.org/10.1057/s41267-021-00468-5>

Mellahi, K., Frynas, J. G., Sun, P., & Siegel, D. (2016). A review of the nonmarket strategy literature: Toward a multi-theoretical integration. *Journal of Management*, 42(1), 143–173. <https://doi.org/10.1177/0149206315617241>

Meyer, K. E., Li, J., Brouthers, K. D., & Jean, R. J. B. (2023). International business in the digital age: Global strategies in a world of national institutions. *Journal of International Business Studies*, 54(4), 577–598. <https://doi.org/10.1057/s41267-023-00618-x>

Microsoft. (2025, February 26). *Microsoft completes landmark EU Data Boundary, offering enhanced data residency and transparency*. <https://blogs.microsoft.com/on-the-issues/2025/02/26/microsoft-completes-landmark-eu-data-boundary-offering-enhanced-data-residency-and-transparency/>

Nambisan, S., Zahra, S. A., & Luo, Y. (2019). Global platforms and ecosystems: Implications for international business theories. *Journal of International Business Studies*, 50(9), 1464–1486. <https://doi.org/10.1057/s41267-019-00262-4>

OECD. (2021). *Trade and cross-border data flows*. https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/06/trade-and-cross-border-data-flows_f54f826e/7bc12916-en.pdf

OECD. (2025). *Economic implications of data regulation*. https://www.oecd.org/en/publications/economic-implications-of-data-regulation_aa285504-en/full-report/component-5.html

Oliver, C. (1991). Strategic responses to institutional processes. *Academy of Management Review*, 16(1), 145–179. <https://doi.org/10.5465/amr.1991.4279002>

OpenSecrets. (2024a). *Alphabet Inc.: Lobbying, 2024 cycle*. <https://www.opensecrets.org/orgs/alphabet-inc/summary?id=D000067823>

OpenSecrets. (2024b). *Apple Inc.: Lobbying, 2024 cycle*. <https://www.opensecrets.org/orgs/apple-inc/summary?id=D000021754>

OpenSecrets. (2024c). *Microsoft Corp.: Lobbying, 2024 cycle*. <https://www.opensecrets.org/orgs/microsoft-corp/summary?id=D000000115>

Reuters. (2018, February 23). Apple moves to store iCloud keys in China, raising human rights fears. *Reuters*. <https://www.reuters.com/article/us-china-apple-icloud/idUSKCN1G70K8/>

Reuters. (2025a, December 1). India orders smartphone makers to preload state-owned cyber safety app. *Reuters*. <https://www.reuters.com/sustainability/boards-policy-regulation/india-orders-mobile-phones-preloaded-with-government-app-ensure-cyber-safety-2025-12-01/>

Reuters. (2025b, December 2). Apple to resist India order to preload state-run app as political outcry builds. *Reuters*. <https://www.reuters.com/sustainability/boards-policy-regulation/apple-resist-india-order-preload-state-run-app-political-outcry-builds-2025-12-02/>

Reuters. (2025c, December 3). India revokes order to preload cybersecurity app on smartphones after outcry. *Reuters*. <https://www.reuters.com/world/india/india-cyber-safety-app-mandate-breach-privacy-main-opposition-party-tells-2025-12-03/>

Siggelkow, N. (2007). Persuasion with case studies. *Academy of Management Journal*, 50(1), 20–24. <https://doi.org/10.5465/amj.2007.24160882>

Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Platform evolution: Coevolution of platform architecture, governance, and environmental dynamics. *Information Systems Research*, 21(4), 675–687. <https://doi.org/10.1287/isre.1100.0323>

Yang, B., & Li, M. (2025). Offshore embeddedness beyond the wall: Chinese cloud providers in Southeast Asia's data governance landscape. *Politics and Governance*, 13, Article 10437. <https://doi.org/10.17645/pag.10437>

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE.

Yoo, Y., Henfridsson, O., & Lyytinen, K. (2010). Research commentary: The new organizing logic of digital innovation. *Information Systems Research*, 21(4), 724–735. <https://doi.org/10.1287/isre.1100.0322>